INFORME ESPECIAL

¿QUIÉN LE ESPÍA?

Ninguna empresa está a salvo del ciberespionaje

"Los ataques de alto nivel dirigidos a empresas están cada vez más generalizados. Miles de empresas ya han sido pirateadas, con el consiguiente robo de sus datos confidenciales y pérdidas económicas que se cuentan por miles de millones. El ciberespionaje es una creciente amenaza tangible y combatirlo es una de las principales tareas que nos hemos fijado".

EUGENE KASPERSKY
FUNDADOR Y DIRECTOR EJECUTIVO DE KASPERSKY LAB

ÍNDICE

"Muchos ciberataques se pueden mitigar tomando medidas relativamente sencillas. Por desgracia, algunas personas no toman ni las precauciones más básicas, como utilizar contraseñas seguras, aplicar parches y ejecutar una solución de seguridad. En muchos casos, acceder a la red de una empresa es más fácil de lo que parece".

COSTIN RAIU
DIRECTOR DEL EQUIPO DE ANÁLISIS E INVESTIGACIÓN GLOBAL
KASPERSKY LAB

¿POR QUÉ TIENE QUE IMPORTARLE A SU EMPRESA EL CIBERESPIONAJE?

RESUMEN

Puede que el ciberespionaje le suene a algo exótico que solo pasa en el cine. Sin embargo, la cruda realidad es que prácticamente cualquier empresa puede ser blanco de esta actividad o salir perjudicada en el fuego cruzado cuando los cibercriminales lanzan un ataque contra otra empresa.

Es irrelevante si su empresa es blanco directo de los ataques o si sufre daños colaterales al verse atrapada en la batalla de otra empresa. De cualquier modo, los resultados pueden ser demoledores.

En este informe, los expertos en ciberseguridad de Kaspersky Lab le ofrecen información sobre los temas siguientes:

- Cómo las empresas pueden sufrir ataques de ciberespionaje directos e indirectos
- Qué puede hacer para proteger a su empresa y la reputación que tanto le ha costado ganar
- Cómo pueden ayudarle tecnologías específicas a defender su red y sus datos corporativos contra amenazas sofisticadas

Los riesgos son una realidad y aumentan tanto en volumen como en sofisticación, pero gracias a los valiosos consejos y a las innovadoras tecnologías de protección de Kaspersky, estará listo para enfrentarse a ellos.

EL ESPIONAJE NO ES NINGUNA NOVEDAD

En una forma u otra, el espionaje ha existido desde que cualquier empresa o individuo ha creído que podría obtener ventajas mediante el acceso ilícito a la información confidencial de otros. Todos conocemos los intentos que varios países han realizado para robar los secretos de otros países. De igual modo, hace mucho que el espionaje industrial forma parte del mundo de los negocios. No obstante, en los últimos años se ha producido un importante cambio en el nivel y la naturaleza de las amenazas de espionaje que pueden afectar a empresas de todos los tamaños.

Hoy en día, la facilidad con la que se pueden implementar las campañas de ciberespionaje tienta a muchas empresas a realizar actividades de espionaje, aunque muchas de ellas jamás se habrían planteado participar en actividades de espionaje industrial a la antigua usanza.

¿QUÉ HA CAMBIADO?

A medida que la era de Internet ha ido ganando empuje y mejorando las posibilidades de conexión y las comunicaciones móviles, las empresas pronto han reconocido las ventajas de ofrecer a sus empleados, clientes y proveedores "acceso en cualquier momento y lugar" a los sistemas y datos fundamentales de la empresa. Las ventajas en cuanto a eficiencia y productividad han sido considerables e incluso han cambiado las reglas del juego para muchas empresas, ya que Internet les ha ayudado a abrir su negocio a nuevos canales de ventas y a generar ingresos adicionales.

No obstante, esta misma conectividad permanente a la información de la empresa y otros datos confidenciales también ha creado oportunidades para los cibercriminales. Como las empresas almacenan propiedad intelectual e información confidencial en sistemas conectados en red, las actividades de espionaje son mucho más fáciles de implementar y pueden resultar mucho más provechosas para sus autores materiales.

EL ESPIONAJE SIMPLIFICADO, CON MÁS RECOMPENSAS INMEDIATAS

Atrás han quedado los días en los que se tenían que forzar las puertas de las oficinas o esperar pacientemente a que contactos internos recopilaran información y transmitieran secretos. Rebuscar en las papeleras de una empresa o pagar a sus empleados para que recopilaran datos siempre resultaba ineficaz, lento y arriesgado. Ahora todo esto es innecesario. Con unos conocimientos adecuados de pirateo informático, individuos y empresas pueden espiar a otras empresas y obtener información valiosa sin tener que salir jamás de la oficina.

Las empresas pueden ser blanco de ataques a inseguridades en su sitio web, vulnerabilidades en software empresarial popular que ejecuten o a consecuencia de los clics de sus empleados en correos electrónicos infectados por malware.

LOS CIBERATAQUES TIENEN CONSECUENCIAS GRAVES PARA LOS RESULTADOS DE UNA EMPRESA

PÉRDIDA MEDIA EN CASO DE UN CIBERATAQUE CON UN OBJETIVO:

2,4 MILLONES DE $

Fuente: Global Corporate IT Security Risks 2013, B2B International

CUANDO LAS EMPRESAS PIERDEN DATOS A MENUDO PIERDEN TAMBIÉN MUCHO MÁS

COSTE MEDIO DE UN INCIDENTE DE PÉRDIDA DE DATOS PARA UNA GRAN EMPRESA:

649 000 $

Fuente: Global Corporate IT Security Risks 2013, B2B International

¿QUÉ OBTIENEN LOS AUTORES MATERIALES DEL CIBERESPIONAJE?

LOS DISTINTOS TIPOS DE ATACANTES TIENEN OBJETIVOS DIFERENTES:

- Los cibercriminales entienden en seguida el valor de la información corporativa. Hay oportunidades de sacar beneficio de campañas de extorsión y rescate, así como de la venta de datos robados en el mercado negro.
- Los activistas hackers se centran en dañar la reputación y dificultar las actividades de las empresas con las que tienen problemas. Se han dado cuenta de que la filtración de información confidencial (sobre clientes, proveedores o empleados) podría conllevar un grave bochorno o sanciones legales importantes.
- Los cibermercenarios se ofrecen al mejor postor (incluidos gobiernos, grupos de protesta o empresas) para robar información concreta.
- Los estados (organismos oficiales) o sus contratistas se centran en recopilar información estratégica o interrumpir las actividades de instalaciones industriales en países enemigos.

"La información es poder. Por tanto, cuando un cibercriminal roba información, el robo puede neutralizar cualquier ventaja de la que disfrute el propietario original de los datos.

Esto es así tanto si el objetivo es un país que tiene secretos militares como si se trata de una empresa con propiedad intelectual y secretos comerciales que le dan una ventaja competitiva".

SERGEY LOZHKIN
INVESTIGADOR EN TEMAS DE SEGURIDAD
EQUIPO DE ANÁLISIS E INVESTIGACIÓN GLOBAL
KASPERSKY LAB

"Empresas de todo tamaño procesan y almacenan datos valiosos para ellas, sus clientes o sus competidores.

Una simple base de datos de información de contacto de clientes ya es valiosa".

PETER BEARDMORE
DIRECTOR SÉNIOR DE MARKETING DE PRODUCTOS
KASPERSKY LAB

¿HAY ALGUNA EMPRESA QUE ESTÉ A SALVO DEL CIBERESPIONAJE?

La respuesta clara es no. Incluso empresas muy pequeñas pueden ser objetivos directos por la información confidencial o valiosa que tienen, desde datos bancarios de clientes hasta información sobre proveedores e incluso datos que se pueden utilizar para contribuir a lanzar un ataque contra una empresa más grande.

Por ejemplo, los ataques contra la cadena de suministro, como IceFog (consulte el Apéndice I), recopilan información de varios organismos o proveedores terceros y luego utilizan esos datos para desarrollar y posibilitar ataques dirigidos a empresas u organizaciones concretas.

"Cuando evalúe los riesgos a los que se enfrenta su empresa, no subestime jamás la posibilidad de que el factor humano debilite sus defensas. Si los empleados resultan ser víctimas de campañas de spear phishing o hacen clic en un enlace infectado en un correo electrónico, su seguridad podría estar en peligro".

SERGEY LOZHKIN
INVESTIGADOR EN TEMAS DE SEGURIDAD
EQUIPO DE ANÁLISIS E INVESTIGACIÓN GLOBAL
KASPERSKY LAB

"Es irrelevante diferenciar entre empresas incluidas en la lista Fortune 500 y empresas de dos personas que trabajen en el garaje de uno de sus padres. Todas tienen algo que perder".

CHARLES KOLODGY
VICEPRESIDENTE DE INVESTIGACIÓN DE PRODUCTOS SEGUROS
IDC

¿ES SU EMPRESA UN OBJETIVO PRIORITARIO?

Es fácil comprender por qué los organismos gubernamentales y militares se encuentran sometidos a ataques de ciberespionaje. Aparte de las iniciativas patrocinadas por estados, los grupos de protesta a menudo intentan interrumpir las actividades del gobierno o robar información confidencial. Los cibermercenarios también eligen como blanco a los organismos gubernamentales para cumplir los objetivos de aquellos que les encarguen el robo de dinero o datos.

De igual modo, puesto que poseen una gran cantidad de información valiosa y tienen reputaciones ganadas a golpe de esfuerzo que deben proteger, las grandes empresas y multinacionales también son blancos obvios de gran cantidad de tipos de ciberataques distintos, incluido el ciberespionaje.

ATAQUES CONTRA GOOGLE, ADOBE Y OTROS

Descrito como un punto de inflexión en la ciberseguridad, el ataque Operación Aurora afectó a Google, Adobe y otras más de 30 empresas destacadas en 2009.

A pesar de los esfuerzos por resolver las vulnerabilidades de software aprovechadas por los atacantes, en 2012 se reveló que este exploit seguía atacando a contratistas de defensa y las cadenas de suministro de empresas de terceros.

El objetivo de los atacantes es tomar el control de sistemas corporativos y robar datos confidenciales. Los sitios web no seguros y las estrategias de phishing por correo electrónico se encuentran en el corazón de lo que se suele considerar ataques de ciberespionaje patrocinados por estados.

ATAQUES CONTRA AMERICAN EXPRESS Y JP MORGAN CHASE

En 2013, American Express y JP Morgan Chase fueron víctimas de ciberataques reivindicados por un grupo religioso. No obstante, expertos en seguridad y agencias de inteligencia estadounidenses creen que el responsable de los ataques fue Irán.

Los ataques hicieron que ambas empresas estuvieran offline durante varias horas.

En el transcurso de seis semanas a principios de 2013, 15 de los bancos más importantes de EE. UU. sufrieron un total de 249 horas de desconexión como resultado de ciberataques.

CUALQUIER EMPRESA PUEDE SER BLANCO DE ATAQUES

Las pymes deben saber que también están en situación de riesgo. Para las pymes, es demasiado fácil desechar las posibles amenazas de ciberespionaje y ciberterrorismo y creer equivocadamente que los riesgos solo afectan a los países y las grandes multinacionales. Esta falsa sensación de seguridad puede hacer que las empresas tengan una actitud demasiado relajada hacia la protección de sus sistemas y datos, lo que puede facilitar la vía a los ciberespías a la hora de lanzar sus ataques.

Además, a menudo los cibercriminales consideran a las pymes como un punto de entrada para ataques contra empresas más grandes. Muchas pymes disfrutan de un estatus de "partner de confianza" de empresas importantes y los delincuentes están cada vez más dispuestos a sacar provecho de esas relaciones.

¿PODRÍA SER SU EMPRESA UN PELDAÑO EN LOS ATAQUES CONTRA TERCEROS?

Los organismos oficiales, ministerios de defensa, propietarios de infraestructuras vitales (como generadores de electricidad, suministradores de gas, redes de distribución de energía y suministradores de agua), además de grandes empresas prácticamente en todos los sectores de mercado, tienen claro que pueden ser objetivos prioritarios de los ciberataques. Por tanto, es probable que todas estas entidades hayan realizado inversiones en fuertes medidas de ciberseguridad.

Por contra, es posible que muchas de las empresas que trabajan con ellas como proveedores o contratistas no tengan conocimientos suficientes sobre el panorama de amenazas moderno ni sobre lo que necesitan para garantizar que van un paso por delante de los ciberatacantes. Obviamente, esto crea oportunidades para que los atacantes accedan a su objetivo prioritario por medio de vulnerabilidades de seguridad en los sistemas de un proveedor o contratista de menor envergadura.

Cualquier empresa, incluidos:

- proveedores de servicios
- proveedores de hardware
- empresas de servicios externalizados
- asesorías pequeñas o unipersonales
- empleados o contratistas temporales

… puede utilizarse como primera etapa en un ataque contra una multinacional o una empresa del sector público.

"A los atacantes les resulta cada vez más difícil acceder a las redes de grandes empresas. Por eso, ahora se centran en la cadena de suministro. Al piratear las redes de empresas más pequeñas, los atacantes pueden aprovechar los conocimientos y las identidades de estas empresas para acceder a empresas más grandes".

COSTIN RAIU
DIRECTOR DEL EQUIPO DE ANÁLISIS E INVESTIGACIÓN GLOBAL
KASPERSKY LAB

LOS ATAQUES CONTRA PROVEEDORES FACILITAN LA POSIBILIDAD DE LLEVAR A CABO UN ATAQUE DIRIGIDO CONTRA UN GRAN FABRICANTE ESTADOUNIDENSE

En 2011, la empresa de defensa estadounidense Lockheed Martin fue víctima de un importante ciberataque.

El autor había atacado con anterioridad a dos de los proveedores de Lockheed Martin, uno de los cuales era RSA (una empresa de seguridad). Se cree que la información recopilada en estos dos ataques ayudó al autor a lanzar su ataque contra Lockheed Martin.

Lockheed Martin detectó rápidamente el ataque y logró proteger sus sistemas y datos. No obstante, este ataque demuestra que se puede utilizar a terceros como peldaños en los intentos de vulnerar la seguridad de grandes empresas.

PÉRDIDA DE REPUTACIÓN

Por descontado, si su empresa solo se utiliza como instrumento para atacar a otra empresa, es posible que no sufra daños directos. No obstante, la posibilidad de sufrir daños indirectos es considerable. Merece la pena tener en cuenta las posibles consecuencias si su empresa se utiliza como el "eslabón débil" que permite un ataque de ciberespionaje contra uno de sus clientes o partners:

- ¿Cómo afectaría a la continuidad de su relación con el cliente o partner?
- ¿Habría consecuencias legales para su empresa?
- ¿Cómo afectaría la publicidad negativa a su reputación en el mercado?
- ¿Podría demostrar que había tomado todas las precauciones posibles contra el ataque?

Claramente, lo mejor es hacer todo lo posible para evitar el bochorno y la pérdida de reputación que podría causar un ataque indirecto.

"Para crear una sólida reputación empresarial, hay que ser tenaz y constante durante mucho tiempo. Perder esa reputación que tanto ha costado ganar puede ser cuestión de minutos".

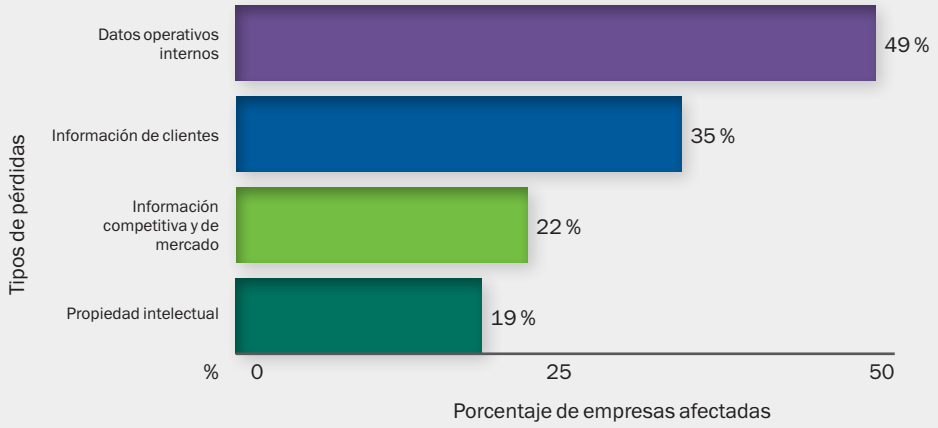
DAVID EMM
INVESTIGADOR REGIONAL SÉNIOR
EQUIPO DE ANÁLISIS E INVESTIGACIÓN GLOBAL
KASPERSKY LAB

PÉRDIDA DIRECTA DE INFORMACIÓN VALIOSA

También merece la pena evaluar el tipo de información que podría estar en situación de riesgo si su empresa pasa a ser el objetivo principal de un ataque de ciberespionaje. ¿Cómo afectaría a su empresa el robo de cualquiera de los siguientes datos?

- Información de mercado, incluida información interna sobre sus puntos fuertes, puntos débiles y posición competitiva.
- Diseños de productos, detalles sobre procesos innovadores, experiencia y otra propiedad intelectual.
- Información personal sobre sus empleados.
- Bases de datos de clientes e información confidencial sobre clientes.
- Información sobre sus partners o datos confidenciales de los mismos.

Una encuesta reciente reveló que las empresas afectadas por fugas de datos experimentaron las siguientes pérdidas:



Fuente: Global Corporate IT Security Risks 2013, B2B International

MÉTODOS DE PROPAGACIÓN DEL MALWARE DE CIBERESPIONAJE

Para distribuir los programas de ciberespionaje, los cibercriminales utilizan muchos de los mismos métodos que emplean para propagar otras formas de malware, como:

- Explotación de vulnerabilidades en sistemas operativos o aplicaciones, incluidos algunos de los productos de software de uso más generalizado, como:
  - o Java
  - o Adobe Reader
  - o Microsoft Office
  - o Internet Explorer
  - o Adobe Flash… etc.
- Técnicas de ingeniería social, incluidas campañas de spear phishing.
- Descargas ocultas, en las que basta con visitar un sitio web con una vulnerabilidad de seguridad para que el equipo del usuario resulte infectado.

EL EFECTO BUMERÁN

Tras la detección e identificación de un nuevo programa de ciberespionaje, podría llegar a pensar que el mundo es un lugar más seguro. Por desgracia, nada podría estar más lejos de la realidad. Los riesgos pueden aumentar y las consecuencias adversas del ataque podrían incluso tener un efecto bumerán y regresar a los autores que lanzaron el ataque inicial.

En algunos casos, otros cibercriminales han copiado los métodos de ataque y se han lanzado nuevos ataques contra el atacante original.

"El concepto que teníamos sobre los ciberataques ha ido cambiando con los años. Lo que parecían ser incidentes aislados (por ejemplo, Stuxnet y Duqu) solo eran la punta del iceberg. En realidad, hay cientos o incluso miles de ataques en marcha en un momento dado, aunque solo se identifiquen unos pocos".

COSTIN RAIU
DIRECTOR DEL EQUIPO DE ANÁLISIS E INVESTIGACIÓN GLOBAL KASPERSKY LAB

MÁS ALLÁ DEL CIBERESPIONAJE LA CIBERGUERRA Y EL RIESGO DE LOS "DAÑOS COLATERALES"

Los actos de ciberguerra, en los que un país lanza ciberataques contra otro país, van en aumento y también pueden tener consecuencias para las empresas.

En las guerras convencionales, "daños colaterales" es el eufemismo que se utiliza para referirse a infraestructuras y civiles que no son objetivos militares, pero que sufren las consecuencias de estas operaciones. En el mundo de las ciberguerras, empresas e individuos inocentes pueden llegar a contarse entre los daños colaterales derivados de un ataque contra otro objetivo.

En cuanto se lanza un ataque de ciberguerra contra un país en Internet, podría tener muchas consecuencias incontroladas o indeseables más allá del objetivo inicial. Los países, las fuerzas armadas y su empresa utilizan Internet. Por consiguiente, si se lanza un ataque de ciberguerra, es posible que empresas inocentes se vean atrapadas en él y que sufran infecciones de malware en sus redes de IT corporativas.
Por ello, cuando se trata de la posibilidad de sufrir daños colaterales, si cualquiera de sus sistemas está conectado a Internet, está en situación de riesgo. Así de fácil.

Además, en caso de producirse un ataque contra la infraestructura vital de un país, aunque los sistemas corporativos de su empresa no queden afectados directamente, también podría sufrir las siguientes consecuencias:

- Pérdida del acceso a almacenamiento de datos y servicios basados en la nube.
- Incapacidad de procesar transacciones financieras online, incluidos el pago a proveedores o empleados o la posibilidad de que los clientes realicen pedidos.
- Problemas de la cadena de suministro, como retrasos en los envíos y en el procesamiento de importaciones o exportaciones.
- Fallos en los sistemas de telecomunicaciones, incluidas las comunicaciones a través de líneas VoIP o LAN.
- Fallos en otras infraestructuras vitales del país, como la generación y distribución de electricidad.
- Pérdida de datos necesarios para actividades de conformidad legal.

¿CÓMO PUEDE PROTEGER A SU EMPRESA CONTRA EL CIBERESPIONAJE?

Aunque algunos de los ataques puedan sonar a cosa de novela de ciencia-ficción, por desgracia, no lo son. Hoy en día, son una realidad y debe protegerse contra ellos.

"Los cibercriminales están dispuestos a aprender nuevas técnicas que puedan mejorar la eficacia de sus ataques. Dedicarán un esfuerzo considerable a la ingeniería inversa de los ataques más sofisticados, incluso los que hayan sido desarrollados por países.

Una vez que el 'genio ha salido de la lámpara' y que hay nuevos métodos de malware 'sueltos', su única esperanza es que su proveedor de seguridad esté en plena forma".

SERGEY LOZHKIN
INVESTIGADOR EN TEMAS DE SEGURIDAD
EQUIPO DE ANÁLISIS E INVESTIGACIÓN GLOBAL
KASPERSKY LAB

EVALÚE LOS RIESGOS Y ESTABLEZCA UNA POLÍTICA DE SEGURIDAD

Es importante que todas las empresas evalúen los riesgos que podrían afectarles y que luego establezcan una política de seguridad propia.

Muchas empresas caen en la trampa de basar su estrategia de seguridad en una percepción anticuada de los riesgos que existían hace 10 años. Por lo tanto, asegúrese de que su política sea relevante para las amenazas actuales y que se base en una sólida comprensión del panorama de amenazas actual. Su política debería:

- Definir los procesos de seguridad diarios.
- Establecer un plan de respuesta a ataques.
- Incluir un mecanismo para actualizar los procedimientos a fin de que sigan el ritmo de la evolución de las amenazas.
- Establecer una rutina para realizar auditorías periódicas de las disposiciones de seguridad de IT.

EXPLIQUE LOS RIESGOS A SU PERSONAL

Es un requisito fundamental. Muchos ataques de ciberespionaje y otros ataques de cibercrimen confían en los errores humanos o en su ingenuidad para crear las condiciones que den a los cibercriminales acceso a sistemas y datos corporativos. Cuando se trata de defenderse contra los ataques, más vale prevenir que curar. Por tanto, asegúrese de dar a conocer:

- Los riesgos de seguridad y los métodos que pueden seguir los cibercriminales para intentar robar información y contraseñas.
- Los posibles costes para la empresa si es atacada.
- Precauciones sencillas que pueden tomar los empleados para mejorar la seguridad.
- La política de seguridad de su empresa y lo que deben hacer los empleados para cumplir sus requisitos.

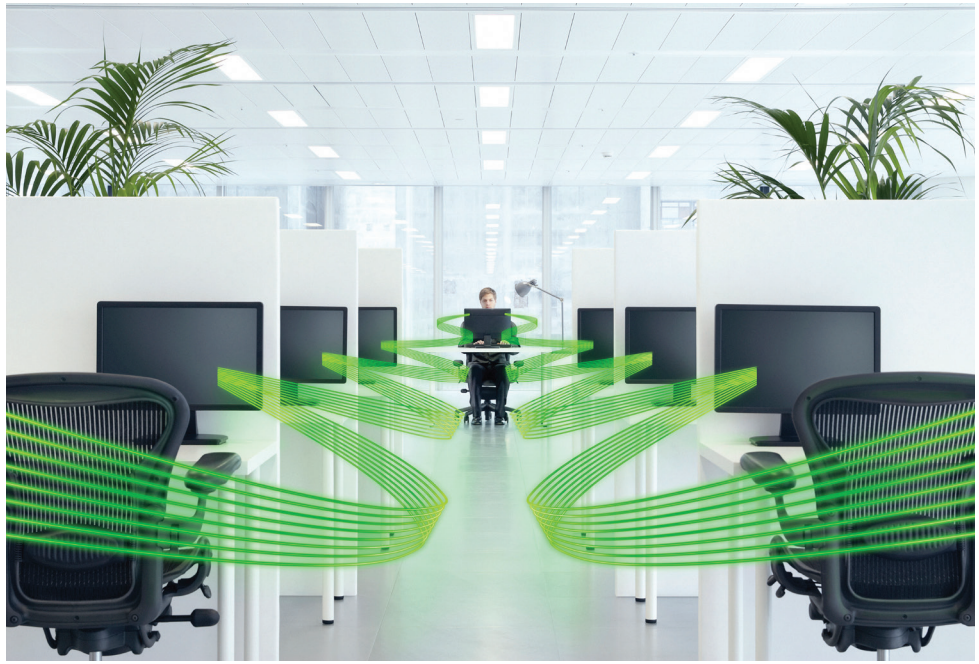
EXAMINE SU ESTRATEGIA EN CUANTO A SISTEMA OPERATIVO

Tenga en cuenta que los sistemas operativos recientes, como Windows 7, Windows 8 o Mac OS X, tienden a ser más seguros que las versiones anteriores. Por tanto, merece la pena tenerlo en mente al planificar la estrategia de actualización de IT.

De igual modo, las versiones de 64 bits de la mayoría de sistemas operativos tienden a ser más resistentes contra los ciberataques.

"Una de las nuevas tendencias que hemos podido observar es aparición de malware destructivo. Un ejemplo sería Shamoon, que se utilizó para atacar a Saudi Aramco y Rasgas en 2012. El malware destructivo se centra en causar el máximo daño a la red de la víctima y, con ello, desactivar su funcionamiento temporalmente o provocar daños irreparables. Esta mentalidad es totalmente distinta de la de los ataques por motivos financieros, como los troyanos bancarios, y quizás incluso es más peligrosa".

SERGEY LOZHKIN
INVESTIGADOR EN TEMAS DE SEGURIDAD
EQUIPO DE ANÁLISIS E INVESTIGACIÓN GLOBAL
KASPERSKY LAB



IMPLEMENTE UNA SOLUCIÓN DE SEGURIDAD DE IT EXHAUSTIVA

La protección antimalware es de vital importancia, pero no es suficiente. Elija una solución de seguridad que también incluya las siguientes tecnologías de seguridad:

- Valoración de las vulnerabilidades
- Gestión de parches
- Controles de aplicaciones que también incluyan marcado en lista blanca y funcionalidad de Default Deny
- Controles de dispositivos que le ayuden a gestionar los dispositivos que tienen permitido conectarse a sus sistemas o redes
- Controles web que faciliten la gestión, restricción y auditoría del acceso a los recursos web
- Defensas contra ataques de día cero aprovechando el poder de la nube para ofrecer una respuesta más rápida a nuevo malware
- Cifrado de datos
- Seguridad móvil con gestión de dispositivos móviles (MDM, del inglés Mobile Device Management)

LA IMPORTANCIA DE LA SEGURIDAD MÓVIL

Los smartphones actuales son mucho más que teléfonos. Son potentes ordenadores que pueden almacenar mucha información corporativa (y contraseñas) que podría ser valiosa para los ciberespías. Por tanto, es importante proteger los dispositivos móviles, incluidos tablets y smartphones, con el mismo rigor con el que protege sus sistemas de IT.

Con el aumento del riesgo de pérdida o robo, lo lógico es que los dispositivos móviles requieran mayores niveles de protección para proteger los datos de los dispositivos perdidos.

Si su empresa ha implementado una estrategia de uso de dispositivos personales en el trabajo (BYOD, del inglés Bring Your Own Device), esto puede agravar sus problemas de seguridad móvil. Asegúrese de tener en cuenta en su política de seguridad la gama casi ilimitada de plataformas y modelos que tendrá que proteger.

CONTROL DE APLICACIONES CON DEFAULT DENY

Default Deny es un método sencillo de gestionar las aplicaciones que se permite iniciar en sus sistemas.

Solo se podrá iniciar el software incluido en la lista blanca de aplicaciones seguras y el resto se bloqueará automáticamente.

Aunque no implemente una política de BYOD formal, debe tener en cuenta que es probable que los empleados lleven sus smartphones personales al trabajo.

PROTEJA SUS ENTORNOS VIRTUALES

Algunas empresas se aferran a la creencia falsa de que los entornos de IT virtualizados son mucho más seguros. No es así. Como las máquinas virtuales se ejecutan en servidores físicos, estos siguen siendo vulnerables a ataques de malware.

Resulta obvio que hay que proteger las máquinas virtuales. No obstante, para mejorar su retorno de la inversión, merece la pena tomar en consideración soluciones de seguridad que incluyan disposiciones especiales para entornos virtuales.

Por ejemplo, si elige una solución de seguridad sin agentes, a diferencia de un paquete de seguridad tradicional basado en agentes, es probable que pueda mejorar los niveles de consolidación de sus servidores.

COMBINE LA SEGURIDAD CON LA GESTIÓN DE SISTEMAS PARA MEJORAR LA VISIBILIDAD Y REDUCIR LA COMPLEJIDAD

Plantéese utilizar una solución que combine la seguridad y una amplia gama de funciones generales de gestión de sistemas de IT. Esto puede ayudarle a mejorar la visibilidad de la red y, si puede ver todo lo que hay en la red, le será más fácil aplicar las medidas de seguridad apropiadas.

"El objetivo de la virtualización es sacar más provecho de la infraestructura de IT. Si ejecuta software antimalware convencional en los servidores virtualizados, podría malgastar gran cantidad de potencia de procesamiento y capacidad de almacenamiento del servidor.

Esto podría frustrar el objetivo del programa de virtualización y reducir significativamente su retorno de la inversión".

DAVID EMM
INVESTIGADOR REGIONAL SÉNIOR
EQUIPO DE ANÁLISIS E INVESTIGACIÓN GLOBAL
KASPERSKY LAB

CÓMO LAS TECNOLOGÍAS DE SEGURIDAD DE KASPERSKY LAB PUEDEN CONTRIBUIR A PROTEGER SU EMPRESA

Como los cibercriminales utilizan métodos cada vez más sofisticados para iniciar ciberataques, es fundamental que las empresas opten por una solución de seguridad capaz de ir al paso de las amenazas más recientes.

TECNOLOGÍAS INNOVADORAS QUE LE OFRECEN DEFENSAS A VARIOS NIVELES

Además de las galardonadas funciones antimalware de la empresa, Kaspersky sigue desarrollando tecnologías innovadoras que añaden más niveles de protección para las empresas:

Análisis avanzado de vulnerabilidades y gestión de parches

Muchas de las soluciones de seguridad de Kaspersky pueden analizar automáticamente su red corporativa para detectar la presencia de vulnerabilidades a las que no se han aplicado parches en los sistemas operativos o las aplicaciones.

Las soluciones de Kaspersky, que funcionan con la base de datos WSUS de Microsoft, la base de datos de vulnerabilidades de Secunia y la exclusiva base de datos de vulnerabilidades de Kaspersky (proporcionada mediante Kaspersky Security Network en la nube), pueden sincronizar con regularidad los datos sobre revisiones y actualizaciones de Microsoft y, a continuación, distribuirlos automáticamente en su red. Además, para muchas aplicaciones que no son de Microsoft, se puede descargar información sobre parches directamente desde los servidores de Kaspersky.

Prevención automática contra exploits (AEP, del inglés Automatic Exploit Prevention)

La tecnología de prevención automática contra exploits de Kaspersky protege contra infecciones de malware que pueden derivarse de vulnerabilidades sin parches aplicados en los sistemas operativos o las aplicaciones que se ejecuten en sus ordenadores.

Kaspersky Security Network

Millones de miembros de la comunidad global de usuarios de Kaspersky se han ofrecido de forma voluntaria para proporcionar datos acerca de actividades sospechosas e intentos de infección de malware producidos en sus ordenadores al sistema Kaspersky Security Network (KSN) basado en la nube. Aunque no participe en el envío de datos a KSN, su empresa se podrá beneficiar de esta afluencia en tiempo real de datos de campo sobre amenazas.

KSN contribuye a ofrecer una respuesta mucho más rápida a nuevas amenazas. Además, también puede reducir la incidencia de "falsos positivos" para que su empresa pueda mejorar la productividad.

Control de aplicaciones

Las funciones de control de aplicaciones de Kaspersky le ayudan a gestionar la manera en que se ejecutan las aplicaciones en su red corporativa. Es fácil configurar una política Default Allow, que bloquea el inicio de aplicaciones incluidas en la lista negra pero permite la ejecución de otro software, o aplicar una política Default Deny, que solo permite iniciar aplicaciones incluidas en la lista blanca.

Laboratorio de marcado en lista blanca

Kaspersky es el único proveedor de seguridad que ha invertido en establecer su propio laboratorio de marcado en lista blanca. El laboratorio se encarga de evaluar la seguridad de las aplicaciones utilizadas habitualmente y emite continuamente actualizaciones de la base de datos de lista blanca de Kaspersky de las aplicaciones cuya ejecución se considera segura.

Las actualizaciones de la lista blanca se ofrecen desde Kaspersky Security Network en la nube, para garantizar que los clientes de Kaspersky se beneficien de los datos más recientes de marcado en lista blanca.

ZetaShield

La tecnología ZetaShield (Zero-Day Exploit and Targeted Attack Shield) de Kaspersky ofrece protección contra malware y exploits desconocidos para defenderse contra ataques de día cero y hora cero, además de contra amenazas persistentes avanzadas (APT, del inglés Advanced Persistent Threats). La combinación del potente motor antivirus y la innovadora tecnología ZetaShield de Kaspersky aumenta considerablemente el índice de detección de malware con el objetivo de ofrecer un nivel de protección más alto, si cabe.

Seguridad móvil y MDM

Las tecnologías de seguridad móvil de Kaspersky ofrecen seguridad a varios niveles para los dispositivos móviles, incluidas funciones especiales para proteger los datos de dispositivos perdidos o robados.

Además, Kaspersky proporciona toda una serie de funciones de gestión de dispositivos móviles (MDM, del inglés Mobile Device Management) que ayudan a las empresas a minimizar el tiempo que deben dedicar a la gestión de endpoints móviles.

Seguridad para entornos virtualizados

Kaspersky ofrece una protección desarrollada especialmente para cumplir los requisitos exclusivos de los entornos de IT virtualizados, como servidores, equipos de escritorio y centros de datos virtualizados.

Al proporcionar una solución antimalware sin agentes, Kaspersky ofrece un método más eficiente para proteger infraestructuras virtualizadas a fin de mantener la estabilidad del rendimiento, minimizar el impacto en la densidad de virtualización y aumentar el retorno de la inversión general.

Funciones de gestión de sistemas de gran alcance

Con la automatización de gran variedad de tareas habituales de administración de IT, Kaspersky Systems Management ofrece a las empresas una mayor visibilidad y control de sus activos de IT y, además, facilita a los administradores de IT más tiempo para dedicarlo a otras tareas.

AUTORIDAD MUNDIAL EN MATERIA DE CIBERSEGURIDAD

Como empresa privada, Kaspersky es totalmente independiente. Aunque Kaspersky asesora a muchos organismos oficiales, no tiene vínculos políticos con ningún gobierno. Los expertos de Kaspersky colaboran estrechamente con la comunidad mundial de seguridad de IT, como los equipos de respuesta a emergencias informáticas (CERT, del inglés Computer Emergency Response Teams) en todo el mundo, y acometen investigaciones conjuntas sobre ciberespionaje, cibersabotaje y amenazas de ciberguerra.

El equipo GReAT de su parte

El equipo de análisis e investigación global (GReAT) es uno de los activos tecnológicos más importantes de Kaspersky. Con investigadores en seguridad líderes en el sector repartidos por el mundo, GReAT analiza constantemente nuevas ciberamenazas y desarrolla protección contra ellas.

"Fundado en 2008, el equipo de investigación y análisis global (GReAT) de Kaspersky Lab lidera la investigación e innovación en antimalware y ciberespionaje, tanto interna como externamente. Los analistas de seguridad del equipo están repartidos por todo el mundo y cada uno de ellos aporta una serie exclusiva de conocimientos y experiencia a la investigación y el diseño de soluciones para combatir código de malware cada vez más complejo.

GReAT realiza la respuesta a incidentes en situaciones relacionadas con el malware. Entre las responsabilidades fundamentales se incluyen el liderazgo de ideas en cuanto a conocimientos sobre amenazas, así como dirigir y ejecutar iniciativas relacionadas con la mejora de la eficiencia y los índices de precisión en la detección de malware y ofrecer asistencia preventa y posventa para cuentas de clientes clave con respecto a la experiencia en conocimientos sobre malware.

En los últimos años, la combinación de experiencia, pasión y curiosidad de GReAT condujo al descubrimiento de varias campañas de ciberespionaje, como Flame, Gauss, Octubre Rojo, NetTraveler e Icefog".

COSTIN RAIU
DIRECTOR DEL EQUIPO DE ANÁLISIS E INVESTIGACIÓN GLOBAL
KASPERSKY LAB

"Con el aumento de las amenazas persistentes avanzadas (APT), el panorama de ciberamenazas mundial se ha transformado, colocando a las infraestructuras vitales, finanzas, telecomunicaciones, institutos de investigación, contratistas militares e infraestructuras de redes informáticas gubernamentales en situación de enorme riesgo.

Estas amenazas son mucho más complejas y sigilosas que el malware habitual. Por todo ello seguimos invirtiendo en GReAT, en la élite de expertos en ciberseguridad de vanguardia".

EUGENE KASPERSKY
FUNDADOR Y DIRECTOR EJECUTIVO
KASPERSKY LAB

COSTIN RAIU
DIRECTOR DEL EQUIPO DE ANÁLISIS E INVESTIGACIÓN GLOBAL
KASPERSKY LAB

Costin Raiu se incorporó a Kaspersky en el año 2000 y ha dirigido el equipo GReAT desde 2010. Está especializado en el análisis de amenazas persistentes avanzadas y ataques de malware de alto nivel. El trabajo de Costin incluye analizar sitios web maliciosos, exploits y malware de banca online.

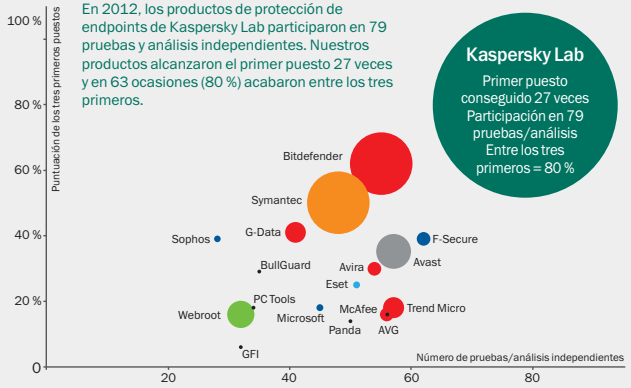
Costin cuenta con más de 19 años de experiencia en tecnologías antivirus e investigación en seguridad y forma parte del consejo asesor técnico de Virus Bulletin, es miembro de CARO (Computer Antivirus Research Organization) e informa para The WildList Organization International. Antes de incorporarse a Kaspersky, Costin trabajó para GeCad como investigador jefe y experto en seguridad de datos con el grupo de desarrolladores del antivirus RAV.

LOGROS Y GALARDONES INDEPENDIENTES

En Kaspersky estamos muy orgullosos de la cantidad de galardones y premios que han cosechado nuestras tecnologías:

- Galardón al proveedor de seguridad de la información del año en la edición europea de los premios de SC Magazine de 2013
- Galardón al equipo de seguridad de la información del año en la edición europea de los premios de SC Magazine de 2013
- Galardón a la excelencia en los premios de SC de 2013
- Kaspersky Endpoint Security for Windows recibió el máximo galardón en la prueba de protección antivirus empresarial de abril – junio de 2013 realizada por Dennis Technology Labs
- El mayor número de galardones de oro y platino (en todas las categorías de pruebas) concedidos por la organización independiente Anti-Malware Test Lab desde 2004
- Más de 50 aprobados en las rigurosas pruebas VB100 desde el año 2000
- El galardón Checkmark Platinum Product de West Coast Labs
- Producto del año, pruebas comparativas AV 2011

KASPERSKY LAB OFRECE LA MEJOR PROTECCIÓN DEL SECTOR*:



*
Notas:
- Según los resultados resumidos de una prueba independiente realizada en 2012 para productos para empresas, consumidores y dispositivos móviles.
- El resumen incluye pruebas realizadas por los siguientes laboratorios de pruebas y revistas independientes:
  - Laboratorios de pruebas: AV-Test, AV-Comparatives, VB100, PC Security Labs, Matousec, Anti-Malware.ru, Dennis Technology Labs.
  - Revistas: CHIP Online, PC Advisor, PC Magazine, TopTenREVIEWS, CNET, PCWorld, ComputerBild, PC-Welt.
- El tamaño de la burbuja representa el número de primeros puestos.

"En 2012, los productos de Kaspersky Lab participaron en 79 pruebas y análisis independientes. Nuestros productos acabaron en 27 primeros puestos y 63 veces entre los tres primeros".

APÉNDICE 1

DESCRIPCIÓN GENERAL DE ALGUNAS CIBERAMENAZAS IMPORTANTES

AMENAZAS DE CIBERESPIONAJE

Icefog

Se trata de una amenaza persistente avanzada (APT) que apareció en 2011 y que se ha dirigido a empresas industriales, organismos oficiales y contratistas militares. La mayoría de los objetivos se encuentran en Japón o Corea del Sur, pero causan problemas en la cadena de suministro a empresas de todo el mundo. Los objetivos de los atacantes suelen ser operadores de telecomunicaciones, operadores de satélites, medios de comunicación y servicios de televisión, así como instalaciones militares, astilleros e instalaciones marítimas, empresas informáticas y de desarrollo de software, y empresas de investigación.

Por lo general, los correos electrónicos de spear phishing se utilizan para transmitir malware que aprovecha las vulnerabilidades de aplicaciones de uso habitual, como Java y Microsoft Office. Aunque las vulnerabilidades sean conocidas y haya parches fácilmente disponibles, los cibercriminales confían en el hecho de que las víctimas pueden ser lentas a la hora de distribuir los parches en su infraestructura de IT. Se cree que los atacantes son cibermercenarios pagados para lanzar los ataques.

Kimsuky

Se sospecha que un grupo de hackers norcoreanos lanzaron la campaña de ciberespionaje Kimsuky para robar datos de defensa y seguridad de objetivos surcoreanos. Los investigadores de Kaspersky Lab descubrieron la campaña que utiliza técnicas de spear phishing para robar las contraseñas y otros datos de los usuarios. Los hackers también se hacen con el control de los ordenadores infectados.

Octubre Rojo

La Operación Octubre Rojo, que se remonta a 2007, todavía estaba activa en 2013. Los objetivos de esta campaña avanzada de ciberespionaje son instituciones diplomáticas y gubernamentales de todo el mundo. También han sido blanco de ella instituciones de investigación, empresas de petróleo y gas y otras organizaciones comerciales. Octubre Rojo roba los datos de sistemas informáticos, teléfonos móviles y redes empresariales. Los ataques incluyen exploits que aprovechan vulnerabilidades de seguridad en Microsoft Office y Microsoft Excel.

NetTraveler

Se trata de una campaña de ciberespionaje que ha logrado afectar a más de 350 víctimas importantes en 40 países. La principal herramienta utilizada por los cibercriminales durante estos ataques es NetTraveler, un programa malicioso usado para la vigilancia informática encubierta. Está diseñado para robar información confidencial, registrar las teclas pulsadas y recuperar listas del sistema de archivos y varios tipos de documentos de Office o PDF. NetTraveler ha estado activo desde 2004 y entre sus objetivos se cuentan activistas tibetanos y uigures, empresas del sector del petróleo, centros e institutos de investigaciones científicas, universidades, empresas privadas, gobiernos e instituciones gubernamentales, embajadas y contratistas militares.

Shamoon

Cuando un ordenador se ve infectado por Shamoon, el virus puede aprovechar la presencia de unidades de disco duro compartidas para propagarse a otros ordenadores en la red de la empresa víctima del ataque. Además de enviar datos al autor del ataque, Shamoon también elimina archivos del ordenador de la víctima.

DATOS BORRADOS DE LOS ORDENADORES DE UN IMPORTANTE PRODUCTOR DE PETRÓLEO

Se cree que un ataque Shamoon destruyó datos de 30 000 ordenadores de Saudi Aramco.

Tanto si su empresa tiene 10 ordenadores como si tiene 10 000, si todos perdieran datos, ¿podría recuperarse del desastre?

AMENAZAS QUE SE CREE QUE SON RESPALDADAS POR PAÍSES, COMO CIBERGUERRA, CIBERSABOTAJE Y CIBERESPIONAJE

Stuxnet (número aproximado de víctimas: más de 300 000)

Stuxnet, que a menudo se considera un ejemplo de ciberguerra, fue el primer programa malicioso dirigido a sistemas de control industrial. El objetivo tras Stuxnet era interrumpir y sabotear el funcionamiento de una planta nuclear, haciéndose con el control del funcionamiento de las centrifugadoras de enriquecimiento de uranio. Hasta la fecha, es el único malware que se sepa que haya causado daños físicos en sistemas industriales.

No obstante, a pesar de su objetivo original, Stuxnet se propagó de manera inestable y ocasionó la infección de cientos de miles de ordenadores en miles de empresas distintas.

Duqu (número aproximado de víctimas: 50 – 60)

Este sofisticado troyano ha estado activo desde 2007. Se creó desde la misma plataforma de ataque que Stuxnet. Tras infectar un ordenador, Duqu descarga componentes adicionales para robar información confidencial. También tiene la capacidad de destruir todas las huellas de su propia actividad.

STUXNET INFECTA A UN GIGANTE PETROLERO

En octubre de 2012, Chevron, un gigante del sector del petróleo, fue la primera empresa con sede en EE. UU. en informar de que había sido infectada por Stuxnet.

Flame (número aproximado de víctimas: 5000 – 6000)

Flame intercepta las solicitudes de Microsoft Windows Update y las sustituye con su propio módulo de malware. El módulo incluye un certificado falso de Microsoft generado por cibercriminales.

Activo desde 2008, Flame puede analizar el tráfico de red de su víctima, tomar capturas de pantalla de sus ordenadores, grabar comunicaciones de voz y registrar las teclas que pulsan los usuarios.

Gauss (número aproximado de víctimas: 10 000)

Implementado por el mismo grupo que creó la plataforma Flame, Gauss es un programa de ciberespionaje que ha estado activo desde 2011. Incluye módulos que pueden realizar varias acciones maliciosas, como:

- Interceptar los archivos de cookies y las contraseñas almacenados en el navegador web de la víctima.
- Infectar dispositivos de almacenamiento USB para robar datos.
- Interceptar datos de cuentas de sistemas de correo electrónico y sitios web de redes sociales.

Gauss se ha utilizado para obtener acceso a sistemas bancarios de Oriente Próximo.

CIBERGLOSARIO

Activistas hackers: a pesar de la ausencia del prefijo “ciber” en su nombre, merecen aparecer en nuestro glosario. Los activistas hackers son hackers informáticos que se han alineado con una organización de protesta o un grupo de activistas concreto. Sus actividades pueden ser parecidas a las de los ciberterroristas o cibersaboteadores.

Armas cibernéticas o ciberarmas: se trata de elementos de malware (software malicioso) desarrollados para dañar a terceros. Las armas cibernéticas se utilizan para ejecutar ataques de ciberespionaje y cibersabotaje. A diferencia de las armas convencionales, las armas cibernéticas son fáciles de clonar y reprogramar.

Ciberataque: ataque realizado por un hacker o un delincuente contra un ordenador, smartphone, tablet o red de IT.

Cibercrimen: se refiere a gran variedad de actividades ilegales implementadas a través de sistemas de IT, incluidos los dispositivos móviles.

Cibercriminal: individuo que realiza actividades delictivas a través de sistemas de IT o dispositivos móviles. Los cibercriminales pueden ir desde delincuentes oportunistas hasta grupos profesionales de hackers informáticos muy capacitados. Los cibercriminales se pueden especializar en:

- Desarrollar malware y venderlo a terceros para que lancen ataques.
- Recopilar datos, como números de tarjetas de crédito, y venderlos a otros delincuentes o llevar a cabo todas las fases de un ataque, desde el desarrollo del malware hasta el robo de dinero a la víctima.

Ciberespacio: área o entorno intangible en el que las redes informáticas de todo el mundo se comunican.

Ciberespionaje: acto de espiar y acceder de manera ilícita a información a través de sistemas de IT o Internet.

Cibergamberro: individuo que desarrolla malware y lanza ataques por diversión. Los cibergamberros, que eran abundantes en las décadas de 1980 y 1990, ya no lo son tanto. En su lugar, los cibercriminales y ciberterroristas son una amenaza mucho más importante.

Ciberguerra: se refiere a ciberataques realizados por países contra otros países. Por lo general, el objetivo de la ciberguerra es dañar infraestructuras propiedad del estado o causar daños mediante el robo de datos confidenciales, en lugar de intentar robar dinero. Los objetivos habituales son instalaciones militares e infraestructuras vitales, como redes de transporte, servicios de control del tráfico aéreo, redes de distribución de electricidad, telecomunicaciones, la cadena alimentaria, etc.

Cibermercenarios: son, como su nombre indica, "hackers a sueldo". De modo parecido a la manera en que el personal de combate profesional ofrece sus servicios a la nación mejor postora durante una guerra convencional, los cibermercenarios son cibercriminales y hackers que venden sus servicios a otros, como países u otras organizaciones.

Cibersabotaje: actividades realizadas por cibersaboteadores para interrumpir procesos o negocios legítimos.

Ciberseguridad: medidas tomadas para defender a los sistemas de IT contra ciberataques.

Ciberterrorista: individuos o grupos que pueden estar respaldados por un estado o actuar como parte de una organización terrorista independiente para lanzar ciberataques.

SOBRE KASPERSKY

Kaspersky Lab es uno de los proveedores de seguridad de IT de mayor crecimiento del mundo y se encuentra entre las cuatro principales empresas de seguridad a nivel mundial. Somos un grupo internacional, operamos en casi 200 países y territorios en todo el mundo y ofrecemos protección a más de 300 millones de usuarios y más de 200 000 clientes corporativos, desde pymes hasta organismos gubernamentales y multinacionales de gran tamaño.

Proporcionamos avanzadas soluciones de seguridad integradas que ofrecen a las empresas una capacidad inigualable de controlar el uso de aplicaciones, Internet y dispositivos; el cliente establece las reglas y nuestras soluciones le ayudan a gestionarlas.

Más información en kaspersky.com/business