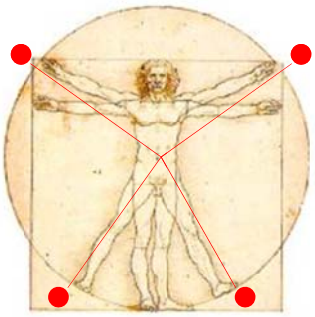
TECNOLOGÍ@ y DESARROLLO

Revista de Ciencia, Tecnología y Medio Ambiente

VOLUMEN XV. AÑO 2017

SEPARATA



RIESGOS DE CIBERSEGURIDAD EN LAS EMPRESAS

Enrique Javier Santiago, Jesús Sánchez Allende

UNIVERSIDAD ALFONSO X EL SABIO
Escuela Politécnica Superior
Villanueva de la Cañada (Madrid)

Marzo, 2017.
http://www.uax.es/publicacion/riesgos-de-ciberseguridad-en-las-empresas.pdf

Escuela Politécnica Superior.
Universidad Alfonso X el Sabio.
28691, Villanueva de la Cañada (Madrid).
ISSN: 1696-8085
Editor: Javier Morales Pérez – tecnologia@uax.es

RIESGOS DE CIBERSEGURIDAD EN LAS EMPRESAS

Enrique Javier Santiago, Jesús Sánchez Allende

a) Doctorando en Ingeniería en Seguridad de la Información, Universidad Alfonso X el Sabio.
Avda. De la Universidad nº1, Villanueva de la Cañada, 28691, Madrid. España.
Enrique.santiago@nst.com.co
b) Doctor Ingeniero de Telecomunicación, Jefe de Estudios de Ingenierías TIC
Escuela Politécnica Superior, Universidad Alfonso X el Sabio.
Avda. De la Universidad nº1, Villanueva de la Cañada, 28691, Madrid. España. jallende@myuax.com

RESUMEN: La tecno dependencia creciente en las organizaciones no solo trae beneficios para las empresas ya que si no se implementan medidas de ciberseguridad y se gestiona el riesgo tanto en la infraestructura tecnológica como en los procesos de negocio, las empresas estarán expuestas a una gran cantidad de amenazas que de aprovechar sus vulnerabilidades podrían comprometer seriamente sus activos de información.
Este documento recopila el resultado de la investigación referente a los riesgos de seguridad a los que se encuentran expuestas las organizaciones actualmente, al igual que el estado del arte de las amenazas digitales, la evolución del malware, las tendencias de los ataques informáticos y nuevos objetivos de las organizaciones cibercriminales como el Internet de las cosas.

PALABRAS CLAVE: Vulnerabilidades, Amenazas, Riesgo, Malware, APT, Internet de las Cosas, BYOD.

ABSTRACT: The Increasing technology dependence of organizations not only brings benefits to organizations else if cybersecurity measures are not implemented and risk is managed in the technology infrastructure and business processes, the companies will be exposed to a large number of threats That exploiting their vulnerabilities could seriously jeopardize their information assets.
This document concentrates the result of research on the security risks to which organizations are currently exposed, as well as the state of the art of digital threats, malware evolution, trends, computer attacks and new targets of cybercrime organizations as the Internet of Things.

KEY-WORDS: Vulnerabilities, Threats, Risk, Malware, Internet of Things, BYOD

1. Introducción

En este artículo se abordan los principales riesgos de seguridad al que están expuestas las empresas del siglo XXI con enfoque descriptivo. Se afronta el riesgo a partir de la relevancia que tienen los activos de información para las organizaciones, se describen los efectos de la tecno dependencia si no se salvaguardan los recursos, el concepto de riesgo y el rol que tienen las vulnerabilidades y las amenazas en la probabilidad de materialización de los incidentes de seguridad como también el impacto que tiene en las organizaciones el compromiso de los activos de información.

Se relacionan también las principales amenazas que afectan el riesgo en las empresas de diferentes sectores. Y se recopilarán una relación de técnicas de ataque empleadas por hackers de sombrero negro para comprometer los activos de información digital de las organizaciones.

Se hace una reseña de las amenazas actuales que hoy en día afectan a la seguridad de la información, la recopilación del estado del arte del riesgo al que se exponen las empresas y las tendencias a las que apunta el mercado que pudieron ser identificadas a partir de las fuentes de referencia y del resultado de la investigación del autor.

El artículo está estructurado en diferentes apartados:

En primer lugar, en el apartado 1 se llevará a cabo una introducción a los riesgos de seguridad a los que están expuestas las empresas.

Para continuar, en el apartado 2 justificando la importancia de la información para las organizaciones. Y se estudian las características que deben salvaguardarse para que pueda considerarse segura dicha información.

En el apartado 3, se describe la tecno dependencia y los efectos no deseados que traen consigo la falta de un sistema o conjunto de procesos de monitorización permanente de los activos de información de la organización. Y se profundizará en por qué este tipo de tecno dependencia incrementa el riesgo para la información corporativa. También se relaciona el rol que tienen los sistemas distribuidos en la operación de los servicios de red LAN y en el mismo internet. También se describe el concepto de superficie de ataque y su relevancia en la medida del riesgo.

Posteriormente en el apartado 4, se relacionan los componentes del riesgo en términos de la probabilidad de materialización de posibles incidentes de seguridad y del impacto que estos representarían para la empresa.

En el apartado 5 se describen los riesgos de seguridad a los que están expuestas las organizaciones. Se explica el origen de las vulnerabilidades en los sistemas computacionales, los tipos de estas. Y se relacionan las principales amenazas involucradas en la materialización del riesgo y los incidentes de seguridad de la información e informática. También se aborda la clasificación del malware y su evolución actual.

En el apartado 6 se estudian los principales ataques informáticos que podrían afectar la integridad, confidencialidad y disponibilidad de los activos de información que se gestionan en las empresas hoy día, el estado del arte de las ciberamenazas y las tendencias.

Posteriormente en el apartado 7 se describen los principales vectores de propagación usados por los agresores para comprometer la seguridad de las organizaciones.

Finalmente en el apartado 8 se muestran las conclusiones obtenidas durante la elaboración de la investigación. Y se realiza una propuesta de trabajo futuro.

Concluiremos con la bibliografía y los recursos de consulta utilizados.

2. Importancia de la Información para las organizaciones

Considerando que toda organización, está compuesta por un conjunto de procesos sinérgicos que se comunican entre sí a través del intercambio de información transformada por cada uno de ellos y que de la completitud, disponibilidad, integridad y calidad de la misma depende el éxito de la operación corporativa al igual que la tomar de decisiones necesarias para dirigir el rumbo de toda compañía; puede afirmarse que la información es el activo más importante de toda empresa y que esta debe hacer todo lo necesario para salvaguardarlo.

Puede afirmarse que la seguridad de la información depende de que se garanticen sus principios fundamentales (Krutz y Vines, 2002, pp. 8-16) conocidos como: la confidencialidad, integridad y disponibilidad al igual que se garantice el no repudio, autenticidad y la trazabilidad de la misma en los procesos en los que se haga uso de ella.

Podría decirse que las medidas de riesgo de la seguridad de la información, los controles que deben usarse para protegerla y la efectividad de los mismos se miden en relación a los principios antes mencionados.

Figura 1: Confidencialidad, integridad y disponibilidad como principios fundamentales de la seguridad de la información.

El termino **Confidencialidad** hace referencia al hecho de que la información sensible de la organización solo pueda ser conocida por personal al que previamente le han sido otorgados privilegios sobre ella. Con el uso de la tecnología, estos permisos de acceso generalmente son asignados a las cuentas de usuario de los empleados para que puedan desempeñar su labor dentro de la empresa.

La **Integridad** se refiere al hecho de que la información solo pueda ser modificada dentro de un proceso corporativo legítimo, durante un periodo de tiempo, desde un sitio autorizado. Y por personal al que la compañía le ha otorgado privilegios. Las adiciones, eliminaciones parciales y cualquier otro tipo de modificación en condiciones distintas a las mencionadas no están permitidas.

La **Disponibilidad** hace referencia a la garantía de que la información sensible de la organización estará accesible por el personal autorizado en el momento en que se considere.

Además, se consideran servicios de seguridad de la información y que deberían ser tratados como características secundarias de la información a aquellos que hacen uso de mecanismos que apoyan el aseguramiento de este activo y se incluyen principalmente a:

El **No Repudio** es un servicio que proporciona la "no renuncia" de la responsabilidad de los actores que participan en una transacción en la cual se haga uso de algún activo de información. Este puede ser No repudio de Origen y/o No repudio de destino y está estandarizado en la ISO-7498-2.

Por otra parte la **Trazabilidad** hace referencia al servicio de registro continuo de las acciones en las cuales esté involucrado cualquier activo de información de la compañía al igual que los datos referentes a los actores participantes, la descripción de la acción ó acciones acompañadas de marcas de tiempo que permitan dentro de un proceso de auditoria reconstruir con detalle el suceso.

Otro servicio importante es el de **Autenticación** que tiene como tarea realizar la verificación de la identidad y los privilegios sobre los activos de información de los actores que pretenden participar en una transacción. De manera que ayuda a facilitar la autenticidad de la información antes de ser procesada dentro de la organización.

La información se considera como la materia prima en la operación de las organizaciones en un mundo globalizado como este, en el que los consumidores se hacen más exigentes. La tecnología es la herramienta clave para reducir los tiempos de respuesta en la atención al consumidor, permitiendo expandir las fronteras del mercado y hacerse cada vez más competitivo.

Por ende, es indudable que, la adopción en crecimiento de la computación dentro de las organizaciones y la interconectividad a la Internet ha demostrado ser elementos claves en la expansión del mercado corporativo, y en el mejoramiento de la calidad de los productos y servicios ofrecidos, facilitando así la competitividad y el crecimiento empresarial. Pero también es claro, que esta situación lleva consigo a la tecno dependencia que sumerge a las empresas en la necesidad de gestionar un nuevo tipo de riesgo; el asociado con la seguridad de su información.

3. Tecno dependencia y su efecto en las organizaciones.

Las organizaciones tienen claro que el uso de la tecnología como apoyo a los procesos de negocio reduce los costos, haciendo más eficiente y eficaz a la operación corporativa. Esta situación puede evidenciarse con el uso masivo del E-commerce y las soluciones de E-banking, tanto web como móviles, que le permiten a los usuarios y cuentahabientes comprar productos y servicios desde la palma de su mano, todo esto gracias a los sistemas distribuidos que son la base de las redes LAN y de la misma internet.

Es obvio entonces, que muchas empresas de este siglo son "tecno dependientes" y esta tendencia es creciente ya que, cada vez más empresarios confían su negocio a la automatización, interconexión computacional y a los procesos en línea.

Pero el uso de la tecnología en los procesos de negocio no solo trae beneficios a las organizaciones y a los usuarios, sino que muchas veces implica riesgos para la información digital, debido a la presencia de vulnerabilidades en el software y hardware computacional, muchas veces resultado de la falta de madurez de algunos productos a nivel de ciberseguridad. De manera que la interconexión a la red de redes no solo

expande el mercado corporativo sino que también expone a los activos de información de estas organizaciones a una gran cantidad de amenazas.

3.1 ¿Porque la Tecno dependencia incrementa el Riesgo?

Tanto los servicios de red como los sistemas de información web y móviles son considerados sistemas distribuidos ya que, están compuestos por tres elementos comunes: un proceso servidor, un cliente y un conjunto de protocolos que son usados para construir mensajes que les permiten a ambos procesos comunicarse y sincronizar sus acciones. Estos elementos describen claramente al modelo Cliente/Servidor en el que se basan todas las aplicaciones usadas en Internet y en las redes LAN que usan la pila de protocolos TCP/IP. En la figura 2 se aprecian estos componentes.

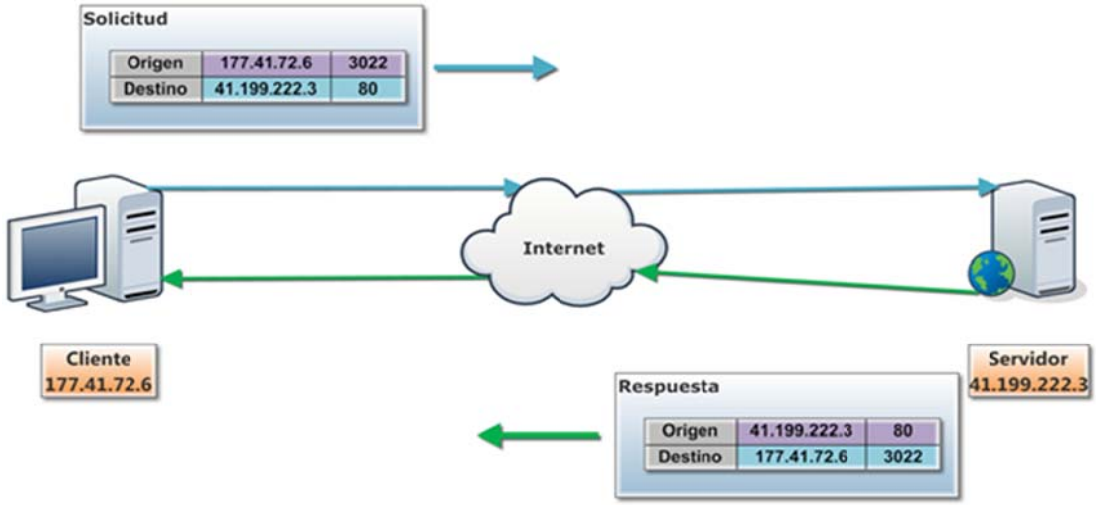


Figura 2: Componentes básicos del modelo cliente / servidor sobre TCP/IP

Los sistemas distribuidos nacieron a mediados de 1970 y tomaron fuerza a finales de 1990, época en la cual no tenía tanta relevancia la seguridad informática como la tiene hoy, de manera que estos y los protocolos que los soportan no fueron construidos pensando en la seguridad de la información, solo se centraban en la funcionalidad. Por esto servicios como FTP, SMTP, POP, TELNET, HTTP entre otros, carecen de protección criptográfica y autenticación fuerte, razón por la cual han sido fácilmente explotados durante mucho tiempo.

Esto hace más complejas a este tipo de soluciones y más susceptibles a fallos de seguridad ya que la sumatoria de los puntos de entrada y salida considerados como la "superficie de ataque"[1] Dr. Partyusa; pueden ser utilizados por un agresor para comprometer los activos de información.

Para los sistemas distribuidos podría considerarse como parte de la superficie de ataque a los siguientes elementos:

[1] Definición dada por el Dr. Pratyusa K. Manadhata en su tesis publicada en http://reports-archive.adm.cs.cmu.edu/anon/2008/CMU-CS-08-152.pdf

- Ordenadores visibles a través de la internet, conectados a la red inalámbrica o desde la misma red LAN
- Routers, Switches, Sistemas PBX.
- Controles de perímetro lógico y físico como firewalls, IPS, IDS.
- Los servicios de capa de aplicación expuestos.
- Los métodos, procedimientos y funciones que expone cada servicio a través de los puertos lógicos.
- Interfaces administrativas
- Funciones de búsqueda y consulta basadas en Formularios.
- APIs, direcciones IP e identificadores de red y Host.
- Recursos de información publicados.

Cuantos más activos/componentes estén expuestos y cuenten con vulnerabilidades explotables, la probabilidad de que una amenaza pueda aprovecharse de estos fallos y materializar el riesgo será mayor, pudiendo afectar la operación de las organizaciones.

La naturaleza misma de los sistemas distribuidos y la necesidad de interoperabilidad de sistemas de diferentes organizaciones a través de tecnologías middleware soportadas por protocolos de comunicaciones no seguros, exponen porciones de código que no solo podrían ser consumidos por sistemas legítimos sino también por hackers maliciosos apoyados por herramientas de Riskware[2] y Malware[3].

La adopción de BYOD "Bring Your Own Device"[4] es otro factor que incrementa el riesgo corporativo afirman algunos investigadores de la Universidad Nacional de la plata, ya que los equipos móviles, asistentes personales de los empleados y visitantes podrían tener vulnerabilidades graves e incluso malware, que una vez conectados a la red corporativa y de no contar esta con unos buenos controles; podrían servir de punto de acceso aprovechable por un agresor para facilitar el compromiso de los activos de información corporativos.

Según el reporte anual de ciberseguridad de la compañía Cisco Systems (Cisco 2017 Annual Cybersecurity Report, 2017)[5], en el 2016 se evidenció la expansión de la superficie de ataque de las empresas que da más espacio para operar a los hackers maliciosos facilitando su éxito, ya que los móviles representan más "Endpoints" que proteger, la integración de la plataforma tecnológica con la Nube expande el perímetro de seguridad que hay que controlar. Y además la creciente integración a la red corporativa de diferentes dispositivos que hacen parte del llamado Internet de las Cosas "IoT" tales como DVRs, cámaras IP, smartTVs, electrodomésticos, weareables y otros elementos de la domótica[6] corporativa como las redes de sensores con las que incluso se forman las smartcities[7] hacen uso de implementaciones de protocolos a los que les falta madures a nivel de ciberseguridad. En el mismo reporte se afirma que el comportamiento de los usuarios sigue haciendo de estos el eslabón más débil de las organizaciones.

[2] http://latam.kaspersky.com/internet-security-center/threats/riskware

[3] https://www.paloaltonetworks.com/documentation/glossary/what-is-malware

[4] Security and Privacy considerations, publico en http://dl.acm.org/citation.cfm?id=2412373.2412741

[5] http://www.cisco.com/c/m/en_au/products/security/offers/cybersecurity-reports.html

[6] http://www.cedom.es/sobre-domotica/que-es-domotica

[7] http://www.creatingsmartcities.es/

4. Riesgo y sus componentes

Según el portal de ISO 27001 en español, el riesgo asociado a la seguridad de la información se define como la "*Posibilidad de que una amenaza concreta pueda explotar una vulnerabilidad para causar una pérdida o daño en un activo de información*". Si consideramos al riesgo como una ecuación, sus variables incluirían la combinación de la probabilidad de ocurrencia de un incidente de seguridad, considerado como una "*serie de eventos de seguridad de la información inesperados o no deseados que poseen una probabilidad significativa de comprometer las operaciones del negocio y amenazar la seguridad de la información.*" y las consecuencias del mismo expresados en términos del impacto producido, donde una vulnerabilidad puede considerarse como una "*Debilidad de un activo ò control que puede ser explotada por una ò más amenazas*" y una amenaza como "*Causa potencial de un incidente no deseado, que puede provocar daños a un sistema ò a la organización.*"

Todo activo de información podría tener por lo menos una vulnerabilidad que podría ser aprovechada por una amenaza. La explotación de esta debilidad da como resultado la materialización del riesgo intrínseco o "propio" del activo de información sin protección alguna.

Una amenaza y una vulnerabilidad por separado no implican riesgo alguno. Es claro que debe existir un activo de información con por lo menos una debilidad al alcance de una entidad que represente peligro o que pueda dañar a dicho elemento. Dicho de otra manera debe existir en el mismo espacio y tiempo un peligro efectivo y un objeto con una debilidad presente que de ser explotada por esa amenaza, pueda dañar al activo de alguna forma. De manera que la materialización del riesgo intrínseco es en sí misma una probabilidad condicional que tomará un valor entre cero (0) y uno (1), dependiendo de la existencia de por lo menos una vulnerabilidad y una amenaza que pueda aprovechar la debilidad presente.

En la figura siguiente pueden apreciarse los componentes del riesgo asociado a la seguridad de la información.

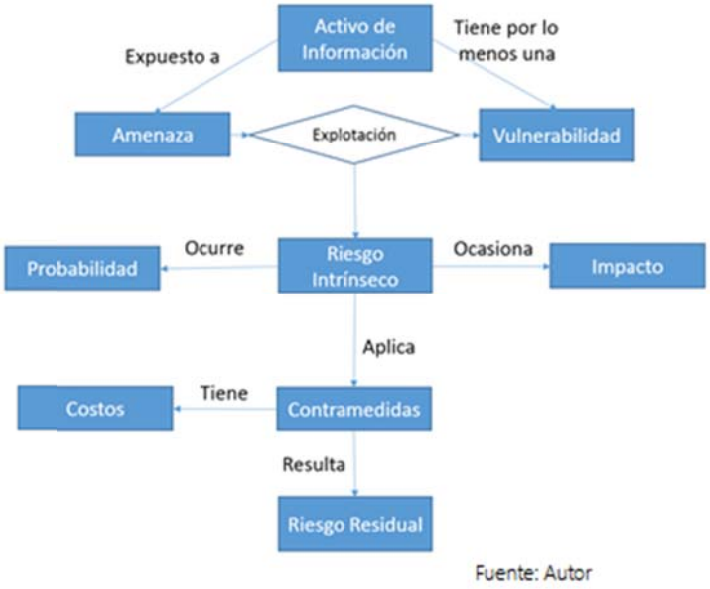


Figura 3: Componentes del riesgo

Entonces, si se considera la presencia de una vulnerabilidad y de una amenaza como dos sucesos independientes, podrían expresarse en términos probabilísticos con la siguiente ecuación:

P(Vulnerabilidad y Amenaza)= P(Vulnerabilidad) x P(Amenaza)

Como el riesgo intrínseco es igual a la probabilidad de que exista una amenaza que pueda aprovechar una vulnerabilidad presente en el activo, entonces:

P(Vulnerabilidad y Amenaza) = P(Riesgo Intrínseco)

Entonces podría representarse a la probabilidad de riesgo intrínseco con la siguiente ecuación:

P(Riesgo intrínseco)= P(Vulnerabilidad) x P(Amenaza)

En el contexto de la seguridad de la información, la probabilidad de la materialización del riesgo intrínseco es equivalente a la probabilidad de la presencia de un incidente de seguridad; de manera que sería válida la expresión:

P(Incidente seguridad)=P(Riesgo Intrínseco);

Entonces:

P(Riesgo intrínseco)= P(Vulnerabilidad) x P(Amenaza)

En el contexto corporativo la materialización del riesgo tiene un impacto en algún proceso del negocio. Mientras más crítico sea proceso o el activo de información afectado, mayor será el impacto de la amenaza.

De manera que la severidad del riesgo de seguridad de una organización es una variable dependiente de la probabilidad de la materialización de un incidente y del impacto del mismo a la organización y podría expresarse con la siguiente ecuación:

Severidad Riesgo = [Probabilidad de un incidente de seguridad] x [Impacto causado]

Las organizaciones cuentan con una herramienta de mucha utilidad para reducir el riesgo al que están expuestas, esta es llamada “Análisis de Riesgos” que a partir de la aplicación de una metodología cualitativa como NIST800P, ISO27005 entre otras, o una cuantitativa como Magerit facilitan la construcción de la “Matriz de Riesgos” de los procesos definidos en el alcance. Dicha matriz de riesgos permite identificar las contramedidas y controles necesarios para salvaguardar sus activos de información. Generalmente las empresas consideran a los costos de los controles y su implementación como un factor importante para la adquisición y puesta en producción de las salvaguardas.

Considerando que el Análisis de riesgos está más orientados a los procesos, es una buena práctica de muchas organizaciones realizar un proceso de identificación, evaluación de vulnerabilidades en el marco de un test de penetración a su infraestructura tecnológica. Estas actividades de hacking ético se apoyan en metodologías como por ejemplo OSSTMM de ISECOM, ISAFF, CEH de ECCouncil y OWASP para el testing de aplicaciones web y móviles.

Al final de la implementación de las medidas de protección y monitorización deben considerarse la construcción de planes de contingencia y de gestión de incidentes para tratar al riesgo residual que podría materializarse a pesar de la presencia de los controles.

5. Riesgos de Seguridad en las organizaciones

La gran mayoría de los componentes tecnológicos que usan todas las organizaciones a nivel mundial tienen vulnerabilidades. Según la compañía CYBSEC Security muchas de estas debilidades pueden nacer con el producto como parte del diseño, tal vez por la omisión de los requisitos mínimos de seguridad de la información que todo nuevo producto software debe cumplir que debe considerarse por el analista de sistemas desde la fase misma de ingeniería de requisitos.

Aunque la mayor cantidad de vulnerabilidades son adicionadas al producto en la fase de implementación y desarrollo del software que incluye la construcción de la aplicación a través del uso de funciones, métodos y procedimientos débiles del lenguaje de programación elegido en el proyecto.

El desarrollo de aplicaciones de muchos fabricantes de software es una carrera contra el tiempo con el fin de sacar al mercado nuevas versiones de sus aplicaciones, que finalmente son productos que deben ser comercializados lo más rápido posible para no perder mercado.

Esta carrera contra reloj, junto con las malas prácticas de ingeniería de software, la ausencia o pobre adopción de metodologías de calidad de software como CMMI[8] más la falta de entrenamiento en "desarrollo seguro"[9] y la concienciación en ciberseguridad, garantiza la presencia de "Bugs" en las aplicaciones, como los errores de división por cero, bucles infinitos, deadlocks, etc. Y omisiones, como la falta de gestión de excepciones, omisión en declaración de tipos de variables, falta de dimensionamiento de las mismas y omisión de funciones de validación de parámetros. Estos hechos conllevan a la aparición de vulnerabilidades en el código fuente que podrían ser explotables.

Estas vulnerabilidades son llamadas "Vulnerabilidades de día Cero"[10] cuando son recién descubiertas y no existe ninguna contramedida para reducir el riesgo que representan. Y muchas de ellas son comercializadas en el mercado negro por hacker maliciosos con ánimo de lucro. Una vez el fabricante o un tercero, desarrollan el parche o código corrector del fallo, y este se publica generalmente por parte de algún Centro de Respuesta a Incidentes (C.E.R.T) entonces pasa a ser una vulnerabilidad común.

En muchas situaciones las vulnerabilidades son el resultado del uso de funciones, métodos y procedimientos de algunos lenguajes de programación que tienen fallos de seguridad como ejemplo de ello la función **strcpy(var1,valor)** para lenguaje C que no valida la cantidad de memoria requerida por la variable destino para poder almacenar el valor que se pasa como parámetro causando un fallo en la disponibilidad de la aplicación por el desbordamiento del buffer. A pesar de ello se siguen incluyendo en libros de referencia empleados en cursos de desarrollo de software, y siguen siendo usadas por desarrolladores profesionales.

Ejemplo de esto, es la vulnerabilidad en el API de PHP[11] descubierta por el investigador de seguridad John Page el día 22 de febrero del 2017 en la plataforma web de la compañía "Easycom" que permite a un agresor realizar un Stack Buffer Overflow afectando la disponibilidad del servicio a través de la red.

[8] https://www.sei.cmu.edu/cmmi/

[9] https://www.owasp.org/images/9/93/Desarrollo_Seguro_Principios_y_Buenas_Practicas.pdf

[10] Definición de Vulnerabilidad de día cero, según ESET, http://www.welivesecurity.com/la-es/2015/02/25/que-es-un-0-day/

[11] Stack Buffer Overflow por vulnerabilidad del API de PHP, https://vuldb.com/es/?id.97277

El problema se hace mayor con los desarrollos de software más grandes como los sistemas operativos. Estos están soportados por un elevado número de paquetes de librerías (shared Objects ò Dynamic Library Link, entre otras) que crecen con cada nueva versión y con cada actualización, siendo desarrollados por diferentes programadores, muchos de estos pertenecientes a pequeñas empresas de software distribuidas en el mundo de manera que en muchas situaciones y a pesar de gran cantidad de desarrollos están documentados, los programadores solo llegan a conocer los nombre de las funciones, procedimientos o métodos y el tipo de parámetros que necesitan para continuar con su desarrollo. Esta situación dificulta la detección de código débil que pueda representar alguna vulnerabilidad explotable.

Además algunos lenguajes de programación e incluso productos de software como motores de Bases de datos incluyen funciones y procedimientos almacenados, por ejemplo XP_CMDSHELL para MSSQL Server, que de estar habilitados, podrían ser usados por un agresor externo para ejecutar comandos peligrosos a nivel del sistema operativo que podrían afectar la seguridad de la información de la organización.

En algunas otras situaciones se adicionan vulnerabilidades en los procesos corporativos durante la configuración e integración de productos de software como resultado de la aplicación de malas prácticas, muchas veces por falta de entrenamiento e incluso de concienciación.

Ejemplo de las vulnerabilidades a las que se exponen los activos de información por la configuración de productos de software por defecto se hizo público en julio del 2015 cuando un grupo de investigadores de seguridad pudo evidenciar la exposición de “600 TBytes de bases de datos expuestas por un fallo en la configuración del motor de bases de datos MongoDB”[12] en versiones anteriores a la 2.4.14 que permiten el acceso desde todas las interfaces de red del host (IP 0.0.0.0) y no permiten el “bind_ip” que permitiría restringir el acceso a través de una IP especifica.

Según el artículo de la empresa Globb Security, el uso de software ilegal en las empresas impacta directamente en su ciberseguridad ya que mucho de este software que generalmente se obtiene de fuentes poco confiables, contiene malware que compromete los sistemas corporativos como resultado de la ausencia de políticas y controles de instalación de software. Este mismo informe confirma que el 25% del software ilegal es usado en sectores financieros como la banca y las aseguradoras, también revela que 26% de los empleados admitieron haber instalado software de fuera de la compañía en los ordenadores de sus empresas.

5.1 Malware

Muchos de los incidentes informáticos que se presentan en las organizaciones son materializados a través del uso de Malware y en otras situaciones con el uso de Riskware. El autor considera al Malware como una herramienta de software construida por un programador malicioso con la cual automatiza uno o más procedimientos de explotación de vulnerabilidades de algunos sistemas con el fin de afectar alguna de las características de los activos de información de su blanco.

Entonces, el software malicioso podría considerarse como una amenaza automatizada por su creador para aprovechar las debilidades de la infraestructura tecnológica de las organizaciones con diversos fines, entre ellos:

[12] Publicación exposición de 600TB de bases de datos https://www.redeszone.net/2015/07/23/600tb-de-bases-de-datos-expuestas-por-un-fallo-de-configuracion-de-mongodb/

- Actividades de espionaje y seguimiento.
- Recolección de datos sensibles y robo de información
- La destrucción de la información y/o la avería de los sistemas objetivo.
- La manipulación y alteración de la información como ocurre con los crímenes financieros.
- El uso de tiempo de CPU para actividades de generación de SPAM, propagación de malware e incluso para replicar ataques contra terceros.
- La toma de control de la infraestructura tecnológica como ocurre con las botnets.

La guía de estudio de la certificación de hacking ético de ECCouncil, define que el software malicioso está formado por las siguientes partes:

- *Vector de infección/ propagación:* Rutina que incluye el código que usa el malware para propagarse, infectar ò distribuirse.
- *Payload:* porción de código que ejecuta la acción maliciosa propósito del malware como la destrucción de ficheros, la apertura de un puerto, el registro de acciones del usuario.

Algunos productos de malware incluyen otros componentes adicionales como el *dropper* encargado de garantizar la propagación y persistencia del código malicioso, u otro componente llamado *Trigger* ò *bomba lógica*, encargada de ejecutar el payload en el momento en el que ocurra un evento como un click del usuario o el cumplimiento de una condición como la llegada de una fecha u hora.

Muchos fabricantes antimalware han clasificado a los diferentes productos de software malicioso de acuerdo al propósito del malware. Considerando que es posible encontrar productos de malware diferentes que tengan el mismo *Payload*, a continuación se presenta la clasificación por familias considerando vectores de propagación comunes:

Virus

Son programas maliciosos que se ejecutan en diferentes tipos de ordenadores y que requieren de un fichero anfitrión para ocultar su código e infectar el sistema víctima, de manera que son ejecutados con el archivo a petición del usuario o del sistema operativo; existen muchas variantes, entre ellas se encuentran:

- *Cavity o viruses*, incluyen su código dentro del área de memoria de otros archivos
- *Virus de Macro*, incluyen su código dentro de rutinas de hojas electrónicas y ofimática
- *Virus de camuflaje*, usan nombres y rutas de componentes del sistema operativo.
- *De Sector de Arranque*, ubica parte de su código en el sector de arranque del disco duro
- *Cluster viruses*, altera la tabla de asignación de archivos del sistema de archivos.
- *Stealth Viruses*, emplean diversas técnicas de evasión para protegerse del antivirus
- *Virus de Encripcion*, que evitan la detección cifrando su código.

Gusanos

Software malicioso que no requiere de un anfitrión para su propagación. Se caracteriza por propagarse a través de la plataforma de red de las organizaciones. Aprovecha los servicios en ejecución y algunos copian su código en el área de memoria leída por los sockets de estos servicios con el fin de ser enviados como parte de los mensajes que intercambian servidores y clientes.

Troyanos

Son productos de malware diseñado para facilitarle al agresor acceso "cubierto" al sistema víctima, generalmente están compuestos por tres elementos:

- *Carrier*: es el componente de fachada y transporte del payload, generalmente sirve de carnada para que la víctima ejecute el producto.
- *Payload*: rutinas de código malicioso que afectan los activos de la información, algunas de ellas pueden dañar ficheros, descargar y habilitar puertas traseras, afectar el sistema de archivos, entre otras cosas.
- *Dropper*: es el componente de software encargado de hacer persistente al código maliciosos, entre sus acciones está el crear entradas en el registro de Windows típicamente en HKLM y sobre Unix/Linux y MacOS registrar como servicio al payload ò crear una entrada en /etc/rc.d/rc.local (por ejemplo sobre distribuciones Linux descendientes de RedHat) para hacer arrancable el malware ante reinicios del sistema.

Spyware

Malware desarrollado para ejecutar tareas de espionaje de las actividades ejecutadas en el sistema comprometido. Muchos de estos productos almacenan el registro de acciones del usuario en un fichero oculto/codificado o cifrado, y algunos otros envían esta información directamente al agresor a través de la red usando protocolos como SMTP/HTTP e incluso el antiguo IRC.

A su vez el spyware puede catalogarse como:

- *Keylogger*: software que espía que registra el keystrokes[13] del usuario clandestinamente.
- *Screenlogger*: tipo de Spyware captura screenshots[14] del ordenador del usuario
- *Videologger*: software espía que graba en porciones de video las actividades del usuario, generalmente utiliza algoritmos de compresión para reducir el espacio de almacenamiento y transporte requerido.

Existen también productos de espionaje que incluyen de forma modular todas las funciones antes descritas. Estos productos se consideran suite de espionaje.

Backdoors

En términos del malware para sistemas TCP/IP, las puertas traseras son rutinas de código que al ejecutarse suben un proceso en la memoria RAM del ordenador victima que posee un módulo de comunicaciones con un numero de puerto lógico del nivel de transporte, a través del cual el agresor podrá tener acceso al sistema comprometido.

Generalmente están embebidos de forma oculta en algunos sistemas de información, como también algunos otros productos de malware los incluyen como parte de su Payload.

[13] Teclear del usuario

[14] Pantallazos del escritorio del ordenador del usuario

Rootkits

Producto de Malware que compromete al sistema operativo a través del reemplazo componentes importantes del mismo o suplantando llamadas e interrupciones al sistema (hooking) y que es capaz de ocultar procesos, ficheros, programas, directorios y archivos de configuración para reducir su detección y la de otros productos de malware que se ejecuten en el sistema víctima.

De acuerdo al nivel en el que operan, los rootkits pueden ser:

- *Hypervisor level:* Modifican la secuencia de arranque y se cargan a si mismos en el hypervisor.
- *Kernel Level:* Adicionan código o reemplazan componentes del kernel original.
- *Aplication Level:* inyectan código malicioso a los programas en la capa de aplicaciones.
- *Library level:* interceptan y reemplazan las llamadas originales librerías del sistema operativo por falsos llamados evitando la detección de los procesos maliciosos
- *Boot loader level*: reemplaza el cargador de arranque por una versión modificada por el agresor.
- Hardware/Firmware level: reemplaza/oculta controladores del hardware o su código.

Spoofeadores

Productos de software usados para falsificar mensajes completos o parámetros de diversos protocolos de comunicaciones usados en redes LAN y en la Internet con el fin de interceptar tráfico de un servicio para capturar información sensible, redireccionarlo a un host malicioso o impedir el acceso a los activos de información.

Hijackers

Herramientas de software usadas para interceptar tráfico y secuestrar sesiones activas de varios usuarios de la plataforma de red de las organizaciones. Dentro de sus métodos de intercepción se encuentran:

- *Session fixation*: asignación de un valor conocido para la sesión del usuario víctima.
- *Session side jacking*: secuestro de sesión apoyado en el uso de sniffers.
- *Browser hijacking:* secuestro de la información de sesión modificando el comportamiento del navegador del usuario víctima.
- *Inyección de código:* envió de código de scripting a la plataforma victima para obtener cookies e información de variables de sesión. Típicamente sobre plataformas web.

Exploits y exploits kits

Los exploits son rutinas de código resultado de la automatización de procedimientos de explotación de vulnerabilidades específicas como el “Buffer Overflow”; estas vulnerabilidades conocidas o de día cero presente en un software particular podrían ser explotadas local ò remotamente. Los exploits kits son productos de software creados para construir, gestionar y lanzar exploits contra la plataforma de red de las organizaciones.

Los exploits son apreciados en el mercado negro y muchos de ellos pueden ser comercializados en darknets como la Deepweb, principalmente los de día cero que podrían alcanzar precios del orden de los USD $6.000.

5.2 La nueva Era del Malware

Hibridos:

El Software malicioso ha evolucionado a partir de la conformación de grupos estructurados de cibercriminales que han optado por el uso de malware especializado y dirigido a algunos sectores como el financiero, de salud y de servicios. Muchas de estas organizaciones compran en las Darknets[15] vulnerabilidades de día cero y exploits que las explotan para posteriormente mejoralos con sus equipos de desarrolladores maliciosos.

Bots

Son productos de malware del siglo XXI, construidos principalmente por programadores contratados por redes de cibercriminales, que tienen características de varias familias de malware como: troyanos, backdoors, rootkits, spyware principalmente y que son usados para tomar el control total de los ordenadores y smartphones infectados con el fin de ponerlos a la disposición de una organización cibercriminal a través de un servidor de C&C[16] (también llamado C2) que es administrado por un hacker malicioso con el rol de "pastor" o encargado de la gestión de los drones o zombies[17].

Figura 4: Proceso de creación de una botnet

En la figura anterior extraída del curso oficial de certificación de hacking ético de la empresa ECCouncil[18] se muestra de forma didáctica tanto el proceso de creación, incremento de la población de ordenadores zombies y la agresión que realizan muchas botnets a través de la Internet.

[15] Termino definido por primera vez por Microsoft para referirse a redes usadas para publicar y distribuir contenido digital de forma anónima

[16] Infraestructura de servidores de comando y control que administran los nodos de una Botnet

[17] Drone/Zombie es un término usado para describir a un ordenador que hace parte de una botnet

[18] http://www.eccouncil.org

RATs/Remote Access Trojan:

Son considerados como la evolución de los troyanos y una fusión de estos con las backdoors o puertas traseras que permiten a agresor establecer una conexión remota (generalmente en reversa) para tener acceso al ordenador comprometido. Muchas campañas APT[19] hacen uso de este tipo de malware para ejecutar actividades de reconocimiento, salto de sistemas de autenticación, descarga y propagación de malware otros productos de software malicioso y acceso a información sensible de las organizaciones.

Ransomware:

Producto de software malicioso con tendencia creciente a nivel mundial, que se caracteriza por hacer uso de criptografía Simétrica y Asimétrica también conocida como hibrida para secuestrar los ficheros de los ordenadores y móviles infectados para luego pedir un rescate por la entrega de la llave criptográfica necesaria para descifrar los ficheros comprometidos, típicamente el pago se solicita en Bitcoins e incluso se le da soporte al usuario en la realización del pago del rescate.

6. Principales ataques informáticos que afectan a las organizaciones

Se considera ataque informático a la acción o conjunto de acciones ejecutadas por uno o un grupo de individuos que pretenden afectar las características de los activos de información de una organización o una persona.

En este orden de ideas, los ataques a los sistemas distribuidos se pueden clasificar de varias maneras, por ejemplo según la característica de los activos de información que se vea afectada, de acuerdo a la capa de la arquitectura TCP/IP que afecta y de acuerdo al componente del sistema distribuido que es impactado.

A continuación se relacionan los principales ataques dirigidos a la plataforma de comunicaciones que hace parte de los sistemas distribuidos.

El **ataque de Hombre en el Medio, MitM ó Sniffing Activo**, es un ataque que se realiza a los protocolos de comunicaciones entre dos host, muy frecuente en redes LAN Ethernet conmutadas en donde el agresor previamente conectado a la red cableada o inalámbrica intercepta el tráfico entre el Gateway y el resto de los ordenadores o entre clientes y servidor por ejemplo a través del envío de mensajes ARP gratuitos que envenenan las tablas ARP de los Host por la ausencia de autenticación. En entornos WAN el MitM podría hacerse efectivo a través de la manipulación de las tablas de enrutamiento, también a través del uso de servidores proxy e incluso como resultado de un proceso exitoso de inyección de código en una aplicación web. Finalmente y sin importar el entorno y la técnica usada, estas acciones terminan en el compromiso de la confidencialidad de credenciales, archivos adjuntos, consultas sql, registros de bases de datos y de todo el tráfico que se envié a través de la red sin ningún tipo de cifrado.

El **Ataque de ARP spoofing**, muy frecuente en las redes LAN Ethernet conmutadas permite que un agresor pueda comprometer la integridad de las tablas ARP usadas por el stack Ethernet y TCP/IP para crear un vínculo entre direcciones IP y MAC; con esta actividad el agresor podría afectar la confidencialidad e incluso la disponibilidad de los servicios.

El **Reply Attack** o **Ataque de repetición** se basa en el reenvió de credenciales cifradas o huellas dactilares previamente obtenidas por el agresor como resultado de un ataque de intercepción al tráfico de autenticación entre un cliente y el servidor legítimo. El agresor no necesita conocer las credenciales en

[19] Advanced Persistent Threats

texto claro, solo reenvía el criptograma o el hash como ocurre por ejemplo con el ataque de repetición sobre sistemas operativos Windows llamado ***Hash Injection,*** en el que se hace uso de la huella dactilar LM HASH, NT HASH con el único fin de iniciar una sesión ilegal en nombre de un usuario legítimo. Con esta agresión se podría comprometer la confidencialidad de la información de la cuenta secuestrada.

Otro ataque que afecta la seguridad de los sistemas de información web es conocido como **HTTP Response Spliting**, y se basa en la manipulación de campo "input" del mensaje HTTP de respuesta adicionando un URL malicioso que podría permitirle al agresor redirigir al usuario victima a este sitio.

Un ejemplo del el mensaje de respuesta manipulado seria el siguiente:

```
Input=usuario_malicioso\r\n HTTP/1.1 200 OK\r\n
```

Ataque de flooding ó inundación. Se clasifican como ataques de inundación a cualquier acción que genere tráfico de uno o varios protocolos que tengan como destinos HOST o equipos de comunicaciones. Uno de los más usados para afectar a las redes LAN y MAN basadas en Metro Ethernet es el MAC FLOOD, que consiste en el envío masivo de tramas Ethernet y Metro Ethernet con direcciones MAC destino y origen aleatorias con el fin de llenar las tablas de conmutación o CAM de los switches.

El ataque Wireless cracking, consiste en la extracción del PassPhrase usado por los protocolos de autenticación de redes WLAN basadas en el estándar IEEE 802.11 como WEP y las variantes de WPA. La técnica usada por el agresor se basa en obligar a los ordenadores de usuarios legítimos conectados a la red Wireless a desasociarse del punto de acceso para posteriormente atrapar copias del tráfico de autenticación que contendrá para protocolos como WEB basados en el algoritmo RC4 un conjunto de vectores de Autenticación que incluirán el deseado PassPhrase. Con las credenciales obtenidas el Host agresor podrá conectarse a la red.

IP y MAC Spoofing son actividades realizada para reemplazar o falsificar una dirección MAC o IP con el fin de dificultar la localización real del host agresor. Existen herramientas como SCAPY del grupo THC, que permiten construir paquetes IP completos con el direccionamiento falsificado y productos como HPING, que pueden recibir la dirección IP falsificada para luego pasarla como parámetro al sistema operativo que la usará para construir un paquete IP legítimo. El IP Spoofing realmente no es un ataque, sino una actividad maliciosa que puede anteceder a un ciberataque tan peligroso como el SYN FLOODING.

El ataque de DNS spoofing, es una agresión que puede ejecutarse usando varias técnicas y que podría comprometer desde un solo host hasta el sistema autónomo de un Internet Service Provider ISP e incluso podría llegar afectar la resolución de nombres de toda la internet. Podría materializarse suplantando la respuesta autoritativa del SOA del dominio a suplantar, envenenando la cache de los STUB DNS Servers, e incluso realizar una transferencia de zona con registros falsificados hacia el DNS Server Secundario.

Ataque de Phishing, esta actividad está asociada con una de las técnicas de la Ingeniería Social orientada al usuario final pero apoyada en tecnología típicamente orientada a la WEB. La materialización de este ataque requiere la ejecución de unas acciones previas como por ejemplo el Pharming o el DNS Spoofing para afectar la resolución de nombres del host victima junto con la puesta en servicio de un servicio WEB en el que el agresor publica una versión falsificada del sitio que de ser visitado por el usuario incauto comprometerá la confidencialidad de sus credenciales de acceso e incluso de sus activos de información.

Campañas APT/ Advanced Persistent Threats

Las Amenazas Persistentes Avanzadas (APT) han demostrado ser el siguiente paso hacia la ciberguerra dirigidas a las empresas y gobiernos, caracterizadas por el uso de técnicas y herramientas de hacking tradicionales usadas por hackers en los 90 pero con una estrategia clara, mayor eficiencia, sofisticación y profesionalismo junto con algunas nuevas herramientas como el software espía, botnets y técnicas de ingeniería social apoyadas por ordenador orientadas a los empleados como el "Spear Phishing". Sus componentes de malware se propagan típicamente a través de redes P2P, de la descarga de torrents y de la suplantación de sitios web; algunas de las más famosas son: ZEUS, Mariposa, GhostNet, Mumba, Stuxnet, Karbanac y Machete.

Las técnicas usadas dentro de las campañas APT y sus productos de malware se caracterizan por la ejecución de tareas de monitorización y ciberespionaje. El resultado de varias investigaciones incluyendo el informe de Kasperky labs sobre el proyecto sauron APT relaciona a gobiernos legítimos como orquestadores de muchos de estos ataques informáticos.

El éxito de estas campañas radica en la ejecución "lenta y suave" de acciones que reducen su detección por parte de los sistemas de defensa tradicionales y la detección de vulnerabilidades explotables en el personal y de día cero en el software.

De manera que el uso de controles de uso común como los firewalls, IPS, sistemas antivirus y pasarelas antiSPAM estándar pierden su efectividad en gran parte por la imposibilidad de identificar la estrategia del agresor por desconocimiento de las acciones maliciosas que impactan a los host vecinos.

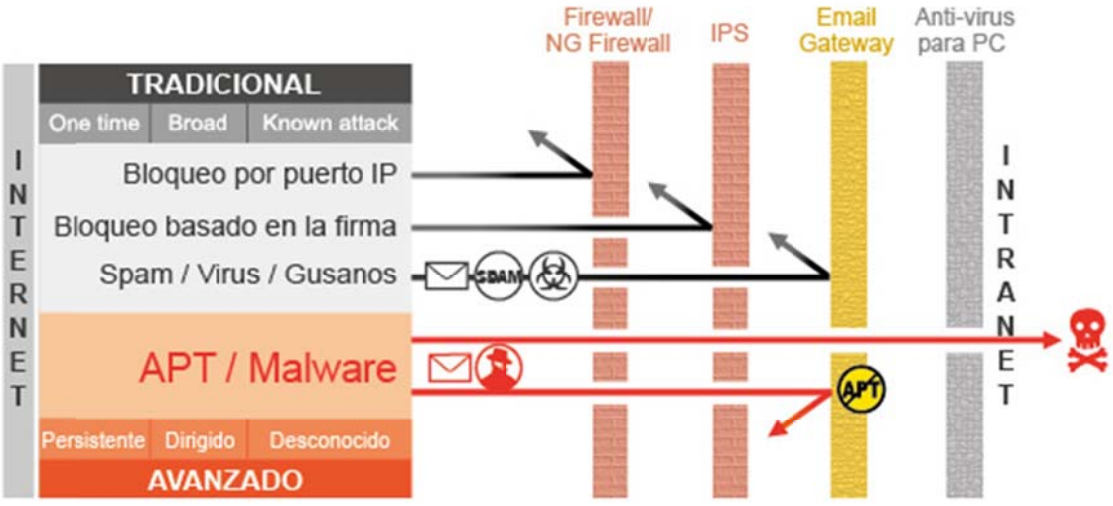


Figura 5: Características de los ataques dirigidos y persistentes.

La figura anterior muestra de forma más didáctica la inefectividad de los sistemas de defensa tradicionales ante las amenazas persistentes avanzadas.

Su acciones se hicieron públicas desde mediados del 2010 pero tomaron mayor fuerza entre el 2012 y el 2015, año en el que algunas Campañas APT han sido las responsables de cortes de energía en instalaciones de generación de energía en Ucrania y en algunos países de medio Oriente.

Ejemplo de estas campañas fue STUXNET descubierta en el 2010 por la empresa de seguridad VirusBlokAda[20] ubicada en Bielorrusia; su bot con características de gusano y software espía fue el primero de su clase con habilidades para reprogramar sistemas industriales SCADA. Todo comenzó cuando los inspectores de la agencia internacional de energía atómica que visitaban una planta nuclear iraní en Natanz, notaron que varias máquinas centrifugas usadas para enriquecer el uranio empezaron a fallar.

Según la empresa de ciberseguridad Symantec en su informe sobre este hecho, El producto de malware probablemente llego a los ordenadores de la planta nuclear a través de un pendrive USB infectado; gracias a sus características de gusano, el bot se propago a través de la plataforma de red hasta localizar el software que controlaba a las centrifugas para posteriormente copiar parte de su código malicioso en él; tomando literalmente el control de estas máquinas.

Una vez insertado el pendrive en la ranura USB del ordenador se inicia la secuencia de propagación del bot copiando unos ficheros temporales al disco duro, posteriormente carga en memoria el primer fichero temporal aprovechando una vulnerabilidad del sistema operativo Windows, luego lleva a cabo una operación de Hooking (técnica utilizada por algunos rootkits para ocultar contenido maliciosos) con el fichero "kernell32.dll", luego repite el proceso con el fichero "Ntdll.dll" e identifica la llamadas a librerías especiales del sistema operativo. Finalmente carga el segundo fichero ejecutable quien recibe el control de la ejecución transformándose en un .dll.

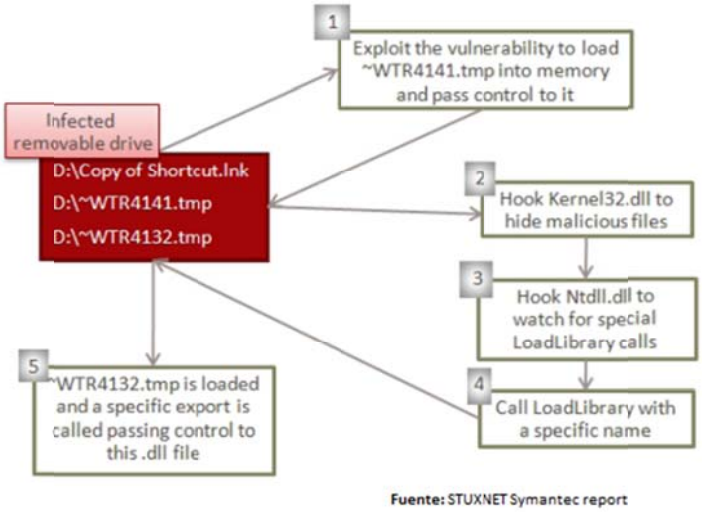


Figura 6: flujo de ejecución vía USB del bot STUXNET

El objetivo final de STUXNET fue infectar los ficheros del controlador lógico programable Simatic (PLC). El código y los datos del controlador de los dispositivos PLC son cargados por bloques a la memoria del ordenador que lo gestiona a través de lenguajes como STL o SCL. El código resultante del proceso de compilación es llamado MC7. Estos bloques de código son cargados en el PLC con el fin de ejecutar, controlar y monitorear el proceso industrial. La librería llamada "s7otbxdx.dll" es la responsable de manejar el intercambio de los bloques de datos entre el PLC y el ordenador con Windows que ejecuta

[20] http://anti-*virus*.by/en/index.shtml

el software de gestión llamado “Simatic manager”. El bot reemplazaba la librería .dll en mención para tomar el control del sistema y reemplazar parte de su código con rutinas maliciosas.

Muchas APT siguen activas, entre ellas pueden citarse a: Poseidon21 Plataforma de Ciberataques compleja que usa backdoors y afecta a sistemas Windows. Adwin22 Plataforma de Ciberataques compleja que usa backdoors y afecta a sistemas Windows/Linux/OS X y Android. Duqu 2,0 se basa en trojanos y afecta a sistemas Windows, BlackEnergy23 Plataforma de Ciberataques compleja que Afecta a sistemas Windows/Linux /Cisco OS. CloudAtlas24 basada en trojanos, afecta sistemas Windows/Linux/ Android/iOS.

6.1 Estado del arte de las amenazas y tendencias a corto plazo

Según el informe “Cyber Threats to the Mining Industry” de Trend Micro después de los efectos nocivos de muchas de las *campañas APT* en varios sectores principalmente en el financiero, y tras ser enfocadas inicialmente al espionaje industrial, estas están siendo reutilizadas y reorientadas para impactar en la disponibilidad de los activos de la industria de la minería, de servicios públicos y otras que hacen uso de sistemas SCADA.

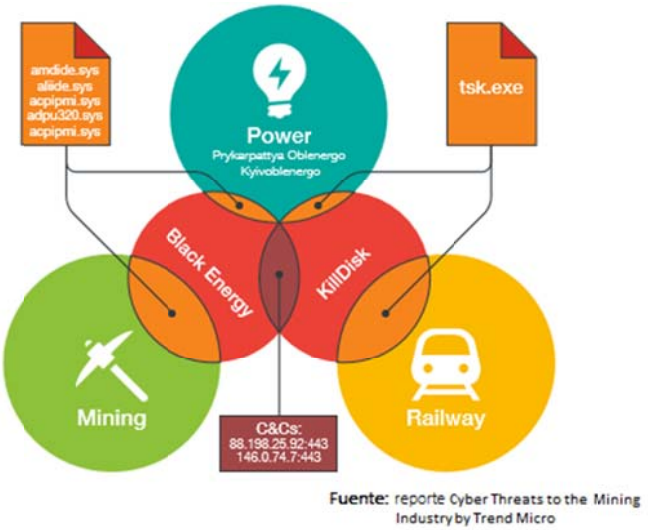


Figura 7: Campañas APT reutilizadas para atacar el sector minero, de energía y ferroviario.

Los sectores objetivos de las campañas APT antes mencionadas son: el eléctrico, el de minería y el de transporte ferroviario, tal como se aprecia en la figura anterior.

Los investigadores de Trend dicen en su informe tener evidencia del uso de herramientas de las campañas: BlackEnergy, SandWorm y Diskkill en la afectación de sistemas de control industrial.

[21] Campaña APT descubierta en el 2015

[22] Campaña APT descubierta en el 2013

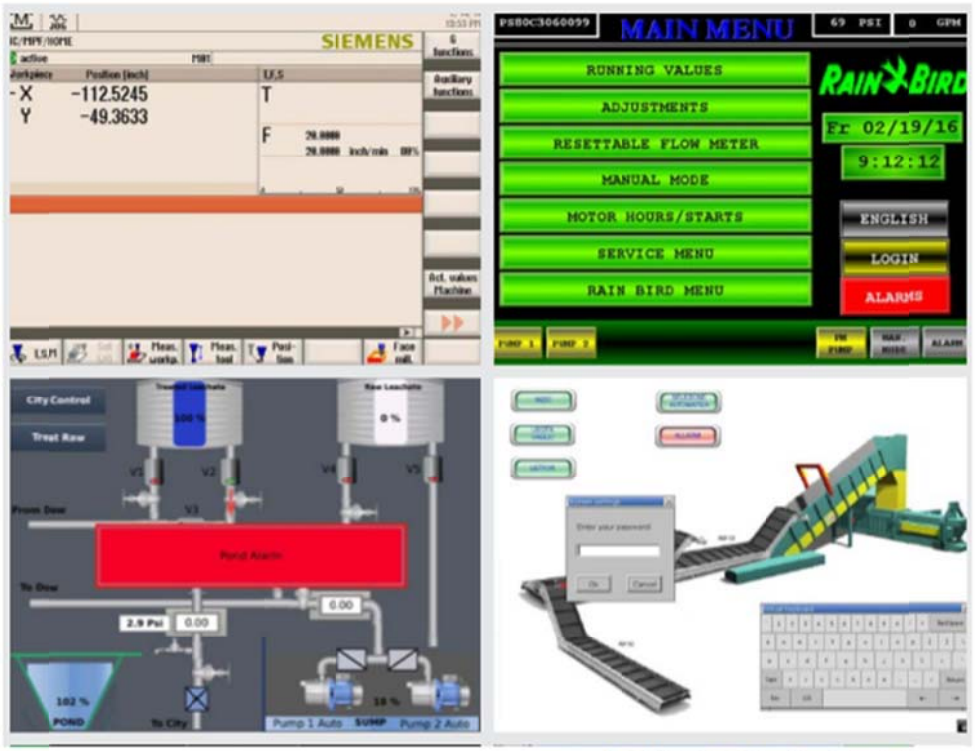
[23] APT Descubierta en el 2013 y que sigue activa

[24] APT descubierta en Agosto del 2014

La industria minera actual cuenta con una infraestructura de comunicaciones que soporta a una red de dispositivos que recolectan, reciben y transmiten información utilizada para garantizar la operación minera. Esta red de comunicaciones alámbrica e inalámbrica no solo interconecta sensores y actuadores sino también ordenadores con información sensible que es potencialmente importante para compañías del mismo sector, para organizaciones gubernamentales y grupos al margen de la ley que comercializan datos robados.

El objetivo de estos ciberataques son el espionaje industrial, el robo de datos referentes a los precios de metales y otros minerales por parte de la competencia a través del uso de hackers contratados; como también la interrupción de la operación minera por parte de grupos Hacktivistas que protestan por el abuso del medio ambiente.

El éxito de estos ataques se debe principalmente escasa implementación y en muchos casos falta de controles de ciberseguridad y al nivel de exposición de muchos de los sistemas computacionales de las empresas mineras en la internet, como se evidencia en la siguiente figura:



Fuente: reporte Cyber Threats to the Mining Industry by Trend Micro

Figura 8: Interfaces Hombre Maquina HMI expuestas en internet.

Con el uso del motor de búsqueda en línea de ordenadores conectados a la internet llamado "Shodan"[25] usado por muchos hackers; un grupo de investigadores de Trend Micro pudieron localizar y tener acceso

[25] Motor del busqueda de ordenadores en linea, https://www.shodan.io/

al software de interface Hombre Maquina de varios sistemas industriales afirman en informe previamente mencionado.

Como ejemplo de este tipo de ciberataques podría mencionarse fue conocida como “el primer ciberataque contra la infraestructura eléctrica de una nación”[26] en diciembre del 2015 que comprometió a 3 compañías eléctricas de Ucrania, dejando sin energía a más de 225 mil viviendas. La intrusión se llevó a cabo desde diferentes fuentes de forma sincronizada logrando el acceso no autorizado a los sistemas de control gracias a la infección previa de varios ordenadores con el software de la campaña APT “BlackEnergy” a través de ficheros de office. Los agresores ejecutaron comandos a nivel de sistema operativo e incluso pudieron hacer uso de un software para control remoto industrial vía VPN.

Según el reporte anual de ciberseguridad de Cisco , Las *Botnet* siguen siendo un peligro creciente para las organizaciones gracias a sus cientos o miles de ordenadores, dispositivos móviles e incluso dispositivos del nuevo Internet de las cosas (IoT). Evidencia de ello fue el ataque de DDOS[27] ejecutado a mediados del mes de octubre de este año, dirigido a la empresa Dyn que provee servicios de resolución de nombres DNS y que alcanzo a dejar inactivos a los servicios ofrecidos por: Twitter,PayPal, Play Station Networks y otras compañías.

El tiempo de CPU y demás recursos de los ordenadores zombies es usado para minar Bitcoins, robar criptomonedas, generar spam, propagar diversos tipos de malware, entre otras actividades como la realización de ataques de denegación de servicios como el antes mencionado.

Según el informe de McAfee labs sobre Amenazas, el robo de información fue uno de los temas principales de su investigación en el 2016, junto con el ransomware y el aprendizaje automático y su aplicación práctica en ciberseguridad.

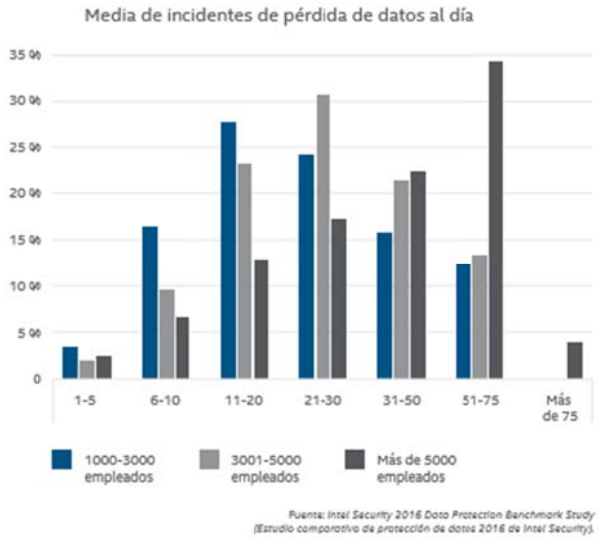


Figura 9: Incidentes perdida de datos según el número de empleados

[26] https://arstechnica.com/security/2016/01/first-known-hacker-caused-power-outage-signals-troubling-escalation/

[27] Ataque de Denegación de servicio distribuido volumétrico o basado en paquetes alterados

Con referencia al robo de datos, McAfee informa que las fugas insignificantes de información y las motivaciones inocentes han quedado en el pasado; la principal motivación de los agresores es el dinero. Según el reporte de "Verizon 2016 Data Breach Investigations"[28] el 89% de las fugas de información fueron provocadas por motivaciones económicas con tendencia al alza desde el año 2013, otra de las razones identificadas fue el espionaje por parte de naciones que desean aumentar su influencia política.

En la figura anterior se aprecia que las empresas más grandes representadas por el mayor número de empleados son las más atractivas para el robo de datos de acuerdo con los resultados de la investigación de "Intel Security" que confirma que la principal motivación es económica.

Por otra parte se ha notado un incremento en el uso de sistemas "Data Loss Prevention" o DLPs, así como al cumplimiento de las normativas referentes a la protección de datos como la LOPD Española y la ley 1581 del 2012 en Colombia, pero aunque el cumplimiento provoca un aumento en la supervisión y la madurez corporativa referente al control de la fuga de información, el "estudio de Benchmark de Intel Security sobre protección de datos del 2016" muestra que el cumplimiento no guarda correlación con la efectividad de las defensas de seguridad ni la prevención de la perdida de datos.

La situación parece indicar que muchas de organizaciones que usan tecnologías DLP trabajan en modo "desatendido" olvidándose de la monitorización. En el informe de Intel antes mencionado se evidencia que el 5% de los profesionales de seguridad encuestados declararon no saber cómo funciona su tecnología de prevención de perdida de datos.

A diferencia de los años anteriores, en el 2016 los principales culpables del robo de datos son los agentes externos entre los que figuran hackers maliciosos, organizaciones cibercriminales e incluso naciones con responsabilidades entre el 60 y el 80% de las fugas reportadas; de manera que entre el 20 y el 40% siguen llevándose a cabo por parte de los denominados "insiders" como los empleados y contratistas tanto de forma intencional como accidental.

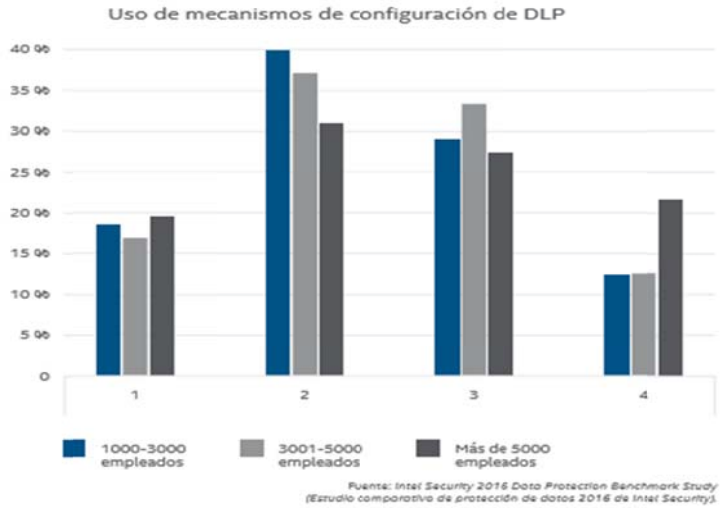


Figura 10: Mecanismos de configuración de los DLP de las empresas según el número de empleados.

[28]Informe sobre robo de información, http://www.verizonenterprise.com/verizon-insights-lab/dbir/

Puede apreciarse en la figura anterior que tanto las organizaciones pequeñas como las grandes hacen uso de la configuración básica en sus sistemas DLP que se basa en expresiones regulares[29]. Estas son efectivas para identificar la fuga de datos estructurados como los que típicamente se usan en las empresas pequeñas pero no tienen la misma efectividad con datos no estructurados como ficheros de texto o de ofimática. Por esto las empresas más grandes generalmente reportan mayor cantidad de incidentes de seguridad referentes a fugas de información.

Con respecto a los datos robados, ha disminuido notablemente los activos de información financiera como las tarjetas de crédito y ha aumentado la fuga de datos médicos y de sanidad, de propiedad intelectual y la información personal, todos estos típicamente en formato no estructurados como hojas electrónicas, documentos de ofimática, de texto y .pdf.

Según McAffe, el proceso de extracción de información sigue basándose en antiguos métodos de hacking, el uso de malware y los ataques de ingeniería social apoyándose con más frecuencia en la información obtenida de medios sociales. La adquisición de los datos sigue realizándose a través de medios físicos. En el 40% de los incidentes reportados se usaron portátiles y pendrives USB. De forma remota los métodos más usados para sacar información de las empresas son a través de protocolos web, de correo electrónico y las transferencias de ficheros.

Compañías como Cisco, McAfee y Kaspersky labs concuerdan en que la amenaza digital más importante del 2016 ha sido el Ransomware quien se ha convertido en un nuevo y lucrativo modelo de negocio para el cibercrimen, que se ha masificado a nivel mundial gracias al incremento de variantes de las cepas más peligrosas que cada día afectan tanto a End Points de escritorio como a servidores, teléfonos móviles inteligentes y hasta SmartTVs, comprometiendo la disponibilidad de los activos de información.

Para la compañía ONA System[30] 50 nuevas familias de Ransomware fueron creadas en los primeros 6 meses del presenta año y en el primer trimestre del año esta amenaza digital generó pérdidas económicas del orden de los 206 Millones de dólares.

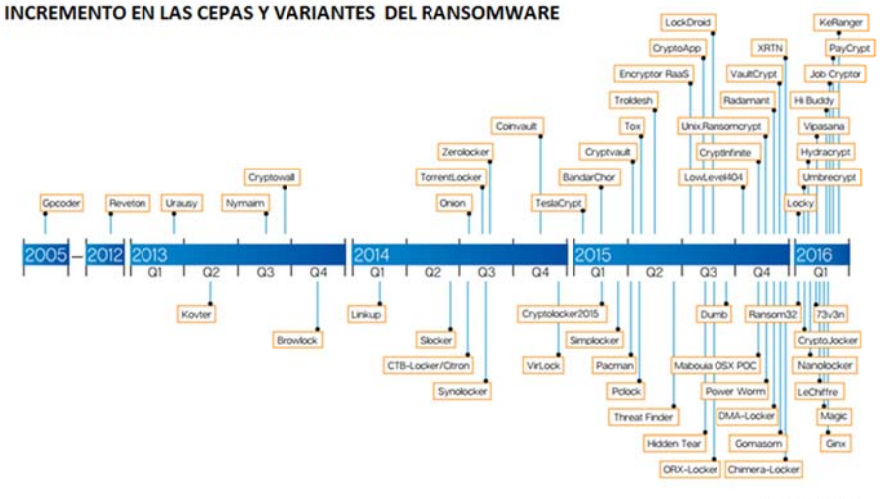


Figura 11: Línea de tiempo del incremento de las cepas de ransomware.

[29] Expresión regular: secuencia de caracteres que define un patrón a buscar

[30] Compañía de ciberseguridad partnet de Intel

Puede apreciarse en la figura anterior extraída del informe de Symantec sobre el crecimiento del ransomware que hay un evidente incremento exponencial en los productos de malware secuestrador desde el segundo trimestre del 2014 hasta finales del 2016.

Su propagación indiscriminada ha impactado en todos los sectores del ámbito corporativo, pero principalmente en las medianas y pequeñas empresas que no cuentan con políticas rigurosas de backup o que sencillamente no poseen copias de seguridad actualizadas de su información. La situación se torna más difícil considerando que aunque los precios de los rescates están entre los 100 y los 20.000 euros (aunque los importes van aumentando a medida que pasa el tiempo), pagar el rescate no garantiza la recuperación de sus datos.

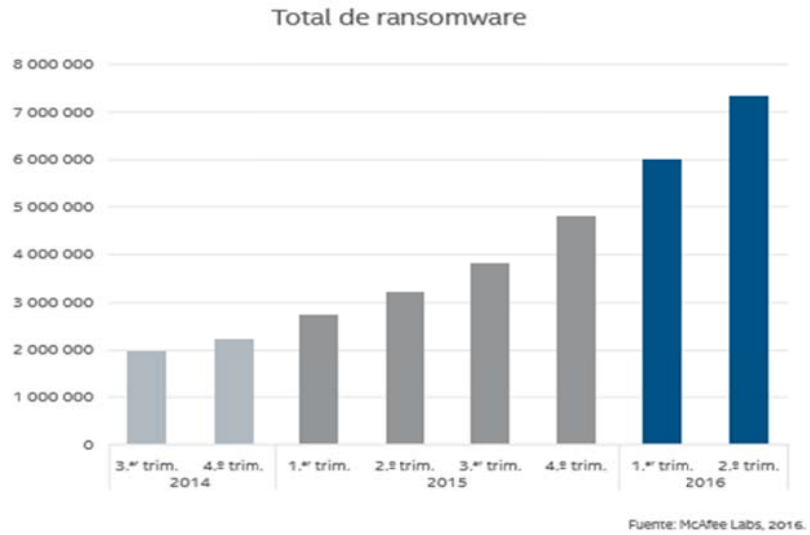


Figura 12: crecimiento del Ransomware a nivel mundial

En la gráfica anterior se aprecia el crecimiento del Ransomware desde el tercer trimestre del 2014 hasta mitad del 2016 según el informe presentado por la empresa McAfee Labs sobre amenazas[31].

Las predicciones para este 2017 no son muy alentadoras según Eset Security en su informe de tendencia para el 2017 titulado "La seguridad como rehén" hace referencia a una modalidad de ransomware llamada por estos investigadores "ransomware de las cosas" o RoT que abre la posibilidad de que los ciberdelincuentes puedan secuestrar dispositivos para luego exigir pago por el rescate que le devolvería el control al usuario. Por otra parte el informe antes mencionado muestra que este tipo de malware seguirá afectando al sector salud tal como lo ha hecho a finales del 2016, esta información coincide con el informe sobre amenazas de McAfee que justifica la situación debido a la falta de soluciones de seguridad, al uso de software anticuado e incluso a dispositivos médicos desactualizados, todo esto acompañado de la necesidad de tener acceso a la información en tiempo real por situaciones en donde se podría ver comprometida la vida de los pacientes. El informe anterior hace referencia a un incidente de ciberseguridad a un proveedor de servicios médicos de Maryland a los que se les pedía una cantidad

[31] Informe McAfee, http://www.mcafee.com/us/resources/reports/rp-quarterly-threats-sep-2016.pdf

importante de Bitcoins[32] por el rescate de los datos; Este proveedor decidió desconectar parte de su plataforma de red para eliminar los mensajes emergentes que recibía cobrando la extorsión; como resultado la atención medica se transtorno ya que no era posible concertar citas médicas, ni consultar registros de sus bases de datos; el resultado fue la interrupción de los servicios médicos de la institución.

Dentro de las tendencias del riesgo para las organizaciones se vislumbra un incremento en los diferentes tipos de ataques, principalmente de denegación de servicio generados por botnets compuestas por DVRs, NVRs, cámaras de video vigilancia IP, sensores y demás dispositivos hechos zombies y controlados por C&Cs[33].

También parece ser factible un incremento en los ataques a las diversas plataformas Cloud orientados al SaaS[34] y a la IaaS[35]

El modelo de negocios que representa el ransomware ha hecho factible la tendencia de del incremento del "Ransomware-As-a-Service" o RaaS, en donde organizaciones cibercriminales desarrollan la plataforma tecnológica incluyendo: sitio web, ejecutable, payload builder, archivos de texto, notas de alerta y la infraestructura para facilitar los pagos en línea en bitcoins. Posteriormente los aspirantes a cibersecuestradores que lo deseen, recibirán el entrenamiento y el acceso a las herramientas dejando como ganancia para la organización criminal una tasa alrededor del 20% de la extorsión. Algunas plataformas como estas ya han sido identificadas, una de ellas es el resultado de un proyecto conocido como "Shark" descubierto por Symantec.

La compañía IBM en su informe titulado "X-force Research 2016 Cyber Security Intelligence Index" revelo que la mayor cantidad de incidentes de seguridad reportados están relacionados con el acceso no autorizado y en segundo lugar con el código malicioso.

7. Métodos de propagación y vectores de ataque

Los principales métodos de propagación utilizados por los agresores para comprometer los activos de información son realmente diversos, podría decirse que los atacantes utilizan cualquier técnica que este a su alcance para materializar la agresión.

Una de los esquemas de infección de malware comúnmente usados en la internet es el *Drive-by-download*. Según el artículo publicado por los investigadores [Takada, Amako] *Drive-by-download* también conocido como (DbD) es llamada así, a la descarga involuntaria de software que proviene de la internet. Podría afirmarse que se refiere a cualquier descarga de software que se hace sin el consentimiento del usuario, generada típicamente por software malicioso ya instalado en el ordenador. Como también se incluyen las descargas autorizadas por el usuario que no tiene claridad sobre sus consecuencias.

Estas descargas no autorizadas podrían darse por ejemplo al hacer click sobre una ventana emergente del navegador, al consultar el contenido de un mensaje de correo electrónico en formato HTML o que contenga algún script, incluso por el simple hecho de visitar un sitio web.

[32] Criptomoneda digital

[33] Servidores de Comando y Control

[34] Software como servicios

[35] Infraestructura como servicio

Javascript sigue siendo usado como vehiculo de infección de sitios web según reporta el portal de noticias de la compañía de ciberseguridad Sophos[36], ya que este lenguaje de script hace parte integral de las soluciones web junto con HTML y las hojas de estilo CSS. Incluso esta misma organización descubrió una nueva variedad de ransomware escrita totalmente en este lenguaje de scripting, gracias a que el sistema operativo Windows permite la ejecución de código javascript y a que su ejecución no genera una alerta de seguridad ni requiere permisos de administrador.

Según informa la Oficina de Seguridad del Internauta – OSI[37], del instituto Nacional de Ciberseguridad (INCIBE) en su servicio antibotnet. Productos recientes de malware como el troyano bancario que apoya a la Botnet "Nercus" que afecta sistemas operativos Windows 7/8/10 utilizan como método principal de propagación el antes descrito.

Otro importante vector de ataque son los Exploits remotos. El mayor éxito de este vector de ataque tiene mucho que ver con la falta de actualización de los productos de software de los equipos de las empresas y de los usuarios que le facilitan a los ciberdelincuentes obtener información de las vulnerabilidades conocidas y algunas veces de día cero de sus potenciales víctimas que facilitan la construcción de este tipo código malicioso.

Hoy en día es fácil conseguir en el mercado negro[38] los llamados exploit Kits, que no son más que un conjunto de herramientas de malware que permiten fácilmente explotar debilidades conocidas con un conocimiento técnico mínimo. Según la empresa Eset Security, estas herramientas hacen parte de un gran negocio de la ciberdelincuencia llamado "Malware as a service" que permiten evadir los sistemas de seguridad y que cualquier agresor puede adquirirse de forma modular con servicio de soporte incluido.

Es muy común que estos Exploit Kits cuenten con una interface de usuario intuitiva que permita su fácil uso a usuarios noveles garantizando a los creadores de estas herramientas un negocio bastante lucrativo.

Muchas de estas herramientas de malware permiten a sus clientes, crear binarios para explotar vulnerabilidades particulares, agregar técnicas de evasión de antimalwares e incluso armar su propia Botnet estableciendo un servidor de Comando y Control (C2) a través del cual enviar correo spam o publicar en los sistemas comprometidos sitios web maliciosos que finalmente le permiten al agresor obtener números de tarjetas de crédito, credenciales y todo tipo de información confidencial para posteriormente sacar provecho propio de ellas o comercializarlas en el mercado negro.

Un ejemplo de estos Exploit kits es "Phoenix"[39], desarrollado por Alex Udakov arrestado en Rusia en el 2013, por desarrollar y comercializar software malicioso. Este producto de software analizaba el Browser de la víctima buscando debilidades explotables incluso en sus plugins, los de Acrobat Reader y el JRE; una vez detectada la vulnerabilidad, el Exploit kit instalaba adware, spyware y software de phising en el sistema víctima.

Un método de propagación que ha demostrado su éxito es el SPAM, en la gráfica siguiente se aprecia el incremento del volumen del tráfico considerado como spam desde el año 2012 entregado por "Composite Blocking List" CBL generado por ordenadores enviando mensajes que contienen malware.

[36] https://www.sophos.com/es-es/security-news-trends/security-trends/malicious-javascript.aspx

[37] https://www.osi.es/es/servicio-antibotnet/info/necurs

[38] http://www.welivesecurity.com/la-es/2016/06/13/cambios-kits-de-exploits/

[39] https://krebsonsecurity.com/tag/phoenix-exploit-kit/

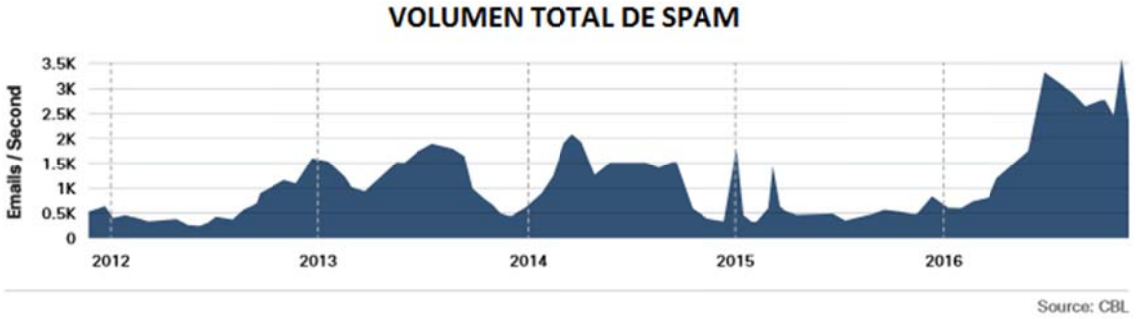


Figura 13: Volumen de tráfico considerado como SPAM en Internet.

El incremento global de este tipo de tráfico que se evidencia en la gráfica anterior parece ser el resultado del incremento del número de zombies de las botnets propagadoras de SPAM, principalmente de la" botnet Nercus". Hoy en día esta botnet es considerada por Cisco en su más reciente informe de ciberseguridad como el vector primario de propagación del ransokmware locky.

Los vectores de ataque y métodos de propagación antes descritos tienen una mayor probabilidad de éxito con el uso de la estrategia que ha demostrado los mejores resultados explotando la confianza del eslabón más débil de la seguridad de las organizaciones, las personas. Esta estrategia es llamada "Ingeniería Social".

8. Conclusiones

En este artículo se ha abordado el riesgo al que están expuestos los activos de información de las empresas en la segunda década del siglo XXI; partiendo de la relevancia de los activos de información considerados como la materia prima de los procesos de negocios y el activo más difícil de recuperar si no se salvaguarda correctamente.

La digitalización facilita el tratamiento de la información, y su procesamiento permite el acceso a nuevo conocimiento que acelera vertiginosamente la competitividad corporativa, al igual que el mejoramiento de los servicios y productos ofrecidos al mercado, y permite que las empresas de esta década puedan predecir las tendencias del mercado y reorientar sus esfuerzos.

La Tecnodependencia implica en sí misma una nueva responsabilidad que debe ser tenida en cuenta por las organizaciones de todo tipo, ya que muchas de las herramientas tecnológicas que se consideran clave para los procesos de negocios, principalmente los de misión crítica o de core de las empresas, tienen embebidas vulnerabilidades que de ser explotadas podrían convertir a la infraestructura tecnológica en un arma de doble filo, que afectarían la disponibilidad, confidencialidad e integridad de los activos de información llegando incluso a paralizar las operaciones y a afectar las finanzas de las empresas.

Después de documentar los principales fallos tecnológicos de la infraestructura computacional de las empresas, es claro que las vulnerabilidades están presentes en casi todos los sistemas tanto a nivel de hardware como de software, y que son el resultado de la omisión de la seguridad de la información en el producto. Bien sea a partir la ingeniería de requisitos, o en las fases posteriores de la ingeniería de software, que incluyen el diseño y la codificación del producto, al igual que la ejecución de las pruebas, la revisión de la declaración de variables, de apuntadores, uso de funciones y métodos vulnerables al igual que la gestión de excepciones principalmente.

Conociendo esta situación ya no solo hackers maliciosos independientes, sino muchas organizaciones cibercriminales están aunando esfuerzos en pro de la explotación de sistemas computaciones y de red a nivel mundial, de empresas de todo tipo, sector financiero y gubernamental, a través del uso de software malicioso cada vez más especializado. Como también, a través de las recientes campañas apoyadas en Amenazas Persistente Avanzadas - APT que son consideradas como la evolución de los ataques informáticos tradicionales. Mimetizándose entre el tráfico de red y de servicios legítimos, llegando a explotar debilidades que ni siquiera el fabricante conoce, llamadas vulnerabilidades de día cero. Otra característica de las APTs es la baja probabilidad de detección por parte de los sistemas AntiMalwalware y típicos controles de perímetro, muchas veces por el uso de riskware en vez del malware tradicional.

Puede observarse a través de esta investigación es el crecimiento del ***CaaS***, o crimen como servicio a través del cual las organizaciones desarrolladoras de malware ofrecen sus productos e infraestructura en modo alquiler para que cualquier persona u organización materialice un ataque contra terceros. Muchos de estos servicios hacen uso de técnicas anti forenses para evitar la judicialización de los agresores. Este tipo de servicios está en crecimiento y ha dado paso al ***RaaS*** o Ransomware como servicio apoyado en kit de herramientas publicadas en la nube que no requieren de conocimientos técnicos avanzados para ser usadas, y que facilitan la extorsión como resultado del secuestro de los activos de información de empresas y personas.

Es claro que el comportamiento del malware tradicional y técnicas de hacking han cambiado y están evolucionando, haciéndose cada vez más difíciles de detectar; el camuflaje y la suplantación, más el uso creciente de técnicas de ingeniería social, hacen que los sistemas de detección y control tradicionales sean inefectivos.

Se considera entonces que existe una necesidad creciente de salvaguardar los activos de información de las empresas debido a la integración de la computación con los procesos corporativos y a la inefectividad de los sistemas de detección y control de amenazas digitales disponibles en el mercado. Por esto el autor considera que es necesario un cambio de paradigma en el proceso de detección de amenazas. A pesar de que existen Sistemas de gestión de eventos de seguridad de la información –SIEMs que realizan correlación de eventos de seguridad, no son adaptativos y carecen de la inteligencia que les permita afrontar nuevas amenazas de forma autónoma sin intervención humana.

9. Bibliografía

AGUILAR Angie, (2015), [En línea]: ¿Qué es y cómo opera un ataque de Cross-Site Scripting (XSS)?, México, pp. 1: [http://www.seguridad.unam.mx/documento/?id=35]

CISCO, (2017), [En línea]: Informe de Ciberseguridad de Cisco 2017, pp. 10-26, [http://b2me.cisco.com/en-us-annual-cybersecurity-report-2017?keycode1=001464170]

COLOURIS George, DOLLIMORE Jean and KIMBERG Tin, (2001): Sistemas Distribuidos: Conceptos y diseño, 3ra Edición, Addison Wesley, pp. 744

CSIRT de la comunidad valenciana (2016), [En línea]: Aparece una nueva versión del APT Duqu, pp. 1, [https://www.csirtcv.gva.es/es/category/tags/apt]

CYBSEC Security Systems, (2007), [En línea]: Seguridad en el ciclo de vida del desarrollo de software, vulnerabilidades en el desarrollo de software, pp. 1-20,[http://www.cybsec.com/upload/cybsec_Tendencias2007_Seguridad_SDLC.pdf]

ECURED, (2016), [En línea]: Conocimiento para todos: Características del gusano informático MYDoom, pp.1,[https://www.ecured.cu/Virus_informático_Mydoom]

ENHACKE, (2016), [En línea]: Ransomware como un servicio altamente lucrativo apunta a acelerarse en 2017, pp. 1,[http://www.enhacke.com/2016/12/19/ransomware-apunta-a-acelerarse-2017/]

ESET, (2017), [En línea]: Tendencias de ciberseguridad Eset Security 2017: La seguridad como rehén, pp. 3-55, [http://www.welivesecurity.com/wp-content/uploads/2016/12/Tendencias-2017-eset.pdf]

GLOBB Security, (2016) [En línea]: El uso de software ilegal en empresas impacta directamente su ciberseguridad, pp.1, [http://globbsecurity.com/software-ilegal]

GOLOVANOV Sergey, (2013), [En línea]: Spyware Analisys: Software RCS Analisys by Kaspersky and exposed in secure list, pp.1 , [https://securelist.com/analysis/publications/37064/spyware-hackingteam]

ISO, (1989) [En línea]: «Estandarización del No Repudio según la ISO como parte de la arquitectura de seguridad propuesta en la ISO-7498-2 », pp. 3. [https://www.iso.org/obp/ui/#iso:std:iso:7498:-2:ed-1:v1:en]

IBM (2016), [En línea]: X-force Research 2016 Cyber Security, pp.1-20,[https://www-01.ibm.com/marketing/iwm/dre/signup?source=mrs-form-2988&S_PKG=ov47123]

INTEL Security, (2016), [En línea]: Data Protection Benchmark Study, pp. 2-25,[https://www.mcafee.com/us/resources/reports/rp-data-protection-benchmark-study-ponemon.pdf]

ISO, (2016), [En línea]: Términos relacionados con ISO 27000 y seguridad de la información: Definición del concepto de Riesgo. pp. 1, [http://www.iso27000.es/glosario.html]

KASPERSKY, (2016), [En línea]: Amenazas para los datos Kaspersky labs: Los tipos de malware, pp.1, [http://support.kaspersky.com/sp/viruses/general/614]

KASPERSKY, (2016), [En línea]: Proyecto Sauron APT, kaspersky labs: Amenaza Persistente Avanzada,pp.3-22,[https://securelist.com/files/2016/07/The-ProjectSauron-APT_research_KL.pdf]

KASPERSKY, (2012), [En línea]: Informe APT FLAME, Kaspersky Labs Análisis de amenazas, pp. 5-84 , [https://securelist.com/files/2015/12/Kaspersky-Security-Bulletin-2015_FINAL_EN.pdf]

KRUTZ, R. L., VINES, R. D. (2002): The CISSP Prep Guide: Gold Edition.
John Wiley & Sons, Inc., New York, NY, USA, pp. 8-11.

MARTINEZ Sergio, (2016), [En línea]: Amenazas a la banca móvil: Malware para los móviles, pp. 1, [http://globbsecurity.com/amenazas-banca-movil-top-10-malware-37372/]

MCAFEE, (2016), [En línea]: Informe sobre amenazas de la empresa McAfee Labs/Intel Security, pp. 6-49,[http://www.mcafee.com/us/resources/reports/rp-quarterly-threats-sep-2016.pdf]

ONASYSTEMS, (2016), [En línea]: Ransomware y sus efectos: Evolución del ransonware, Colombia, pp.1, [http://www.onasystems.net/derrotando-el-ransomware/]

ORIYANO Sean-Philip, (2014), Certified Ethical Hacker study guide, Volume 8, Sybex, Indiana, pp. 352–404.

OWASP. (2014), [En línea]: Top 10 2013-A3-Cross-Site Scripting (XSS), EEUU, pp.1, [https://www.owasp.org/index.php/Top_10_2013-A3-Cross-Site_Scripting_(XSS)]

SYMANTEC, (2010), [En línea]: Informe APT Stuxnet, Symantec Security Response: Análisis de STUXNET, pp.2-68 , [https://www.symantec.com/content/en/us/enterprise/media/security_response/whitepapers/w32_stuxnet_dossier.pdf]

TANENBAUM Andrew S. and VAN RENESSE Robbert, (1985), Distributed Operating Systems. ACM Computing Surveys (CSUR), Volume 17, Issue 4. MIT Press, Pags. 419-470.

TETSUJI Takada , KATSUHIRO Amako, (2015), [En línea]: A Visual Approach to Detecting Drive-by Download Attacks, ACM Computing Surveys (CSUR) Tokyo, Japan. [http://dl.acm.org/citation.cfm?id=2801070&CFID=736718060&CFTOKEN=13646926]

TRENDMICRO, (2015), [En línea]: Security-intelligence cyber threats to the mining industry,pp.1-46,[http://www.trendmicro.com/cloud-content/us/pdfs/security-intelligence/white-papers/wp-cyber-threats-to-the-mining-industry.pdf]

VENOSA Paula, MACÍAS Nicolás, (2016) [En línea]: Dispositivos móviles y el fenómeno del BYOD: Su impacto en la seguridad de las organizaciones, pp. 1-10 [http://sedici.unlp.edu.ar/bitstream/handle/10915/56375/Documento_completo.pdf-PDFA.pdf?sequence=1]