IV FORO DE LA CIBERSEGURIDAD

14 OCTUBRE 2015

CSC Cyber Security Center

Una iniciativa de :

isms forum spain

ASOCIACIÓN ESPAÑOLA PARA EL FOMENTO DE LA SEGURIDAD DE LA INFORMACIÓN

Patrocinan:

Akamai · BLUE COAT · Deloitte. · intel Security · IBM · SAMSUNG · Symantec. · NECSIA · TREND MICRO

Colaboran:

Obra Social "la Caixa" · apd Asociación para el PROGRESO de la DIRECCIÓN el saber conecta

ISMS FORUM SPAIN

La Asociación Española para el Fomento de la Seguridad de la Información, ISMS Forum Spain, es una organización sin ánimo de lucro fundada en enero de 2007 para promover el desarrollo, conocimiento y cultura de la Seguridad de la Información en España y actuar en beneficio de toda la comunidad implicada en el Sector.

Creada con una vocación plural y abierta, se configura como un foro especializado de debate para empresas, organizaciones públicas y privadas, investigadores y profesionales donde colaborar, compartir experiencias y conocer los últimos avances y desarrollos en materia de Seguridad de la Información.

ISMS Forum Spain tiene ya a más de 130 empresas asociadas y más de 850 profesionales asociados.

La Asociación organiza su actividad a través de distintas iniciativas, que abordan desde una perspectiva global o especializada la Seguridad de la Información: Jornadas Internacionales, Data Privacy Institute, Cloud Security Alliance, Cyber Security Center, Centro de Estudios en Movilidad, el portal Protegetuinformacion.com, workshops sobre materias concretas y actividades de formación. Además gestiona las certificaciones Certified Data Privacy Professional (CDPP) y Certificate Of Cloud Security Knowledge (CCSK) en castellano para España y Latinoamérica.

CENTRO DE ESTUDIOS EN CIBERSEGURIDAD

El Centro de Estudios en Ciberseguridad (CEC) es una iniciativa de ISMS Forum Spain creada en 2011 cuya misión es fomentar el intercambio de conocimientos entre los principales actores y expertos implicados en el Sector, para impulsar y contribuir a la mejora de la Ciberseguridad en España.

El CEC quiere crear un estado de conciencia para controlar y gestionar los riesgos derivados de la dependencia actual de la sociedad respecto a las Tecnologías de la Información y la Comunicación (TIC), siendo un aspecto clave para asegurar el desarrollo socio-económico del país.

Para alcanzar la misión anteriormente descrita, el CEC lleva a cabo una importante labor de análisis (estudios), concienciación (eventos) y formación, entre otras actividades relacionadas con la ciberconcienciación.

PROGRAMA

10.00 HS	**REGISTRO**
10.20 hs Bienvenida y presentación.	**Palabras de bienvenida.** **CARLES SOLÉ, Director del Centro de Estudios en Ciberseguridad.**
10.30 hs Ponencia inaugural.	**The power of hacking in businesses.** **A new Cyberlandscape.** **ERKA KOIVUNEN, Former head of Finnish national Computer Security Incident Response Team, CERT Finland; Cyber Security Advisor, F-Secure.**
11.00 HS	**COFFEE BREAK**
11.25 hs Talleres prácticos.	**Talleres prácticos. Análisis y gestión de nuevas amenazas. Deconstrucción y análisis de un ataque DDoS.** 11.25-11.45hs **FEDERICO DIOS, Service Line Manager, Akamai.** **El back door universal.** 11.45-12.05hs **ALBERTO CITA, SE Manager, Southern Europe, Blue Coat.** **Overview of an active banking malware.** 12.05-12.25hs **RENAUD BIDOU, SEUR Technical Director, Trend Micro.** **Cryptolocker: ¡La pasta o la info!** 12.25-12.45hs **CARLOS FERNÁNDEZ, Cybersecurity Technical Leader, Symantec.**
12.45 hs Ponencia	**La Seguridad es tan robusta como su eslabón más débil.** **EMMANUEL ROESELER, Security Systems Sales Manager Spain, Portugal, Israel and Greece, IBM Software.**
13.05 hs Mesa redonda.	**¿Ciberseguridad sin Continuidad?** **ALFONSO MARTÍNEZ, Experto en Resiliencia, Intel Security.** **MANUEL SICILIA, Jefe de la Sección de Análisis del Servicio de Ciberseguridad y OCC, CNPIC.** **ENRIQUE RÍOS, Jefe de Planificación del departamento de seguridad corporativa, Abertis.** **RODRIGO JIMÉNEZ, Security advisor, Necsia.** **Modera: JAVIER CARMONA, Director de Seguridad de la Información y Comunicaciones, Iberdrola.**

14.00 HS	COCTAIL ALMUERZO
15.30 hs Mesa redonda.	**Ciberseguridad en movilidad e IoT.** **RAFAEL SANTOS, Miembro del Comité Operativo, Centro de Estudios en Movilidad; Jefe de Área de Seguridad Informática de la Subdirección General de Tecnologías de la Información y Administración Electrónica, Ministerio de Fomento.** **PALOMA LLANEZA, Miembro del Comité Operativo, Centro de Estudios en Movilidad; Socio-Director, Razona Legaltech.** **JESÚS M. DOMÍNGUES, Miembro del Comité Operativo, Centro de Estudios en Movilidad; Enterprise Business Team Security Solutions, Samsung Electronics Iberia.** **RAÚL SILES, Founder & Senior Security Analyst, DinoSec.** **Modera: FERNANDO PICATOSTE, Socio, Deloitte.**
16.30 hs Demostración de hacking en directo.	**Tres amenazas móviles modernas: el bueno, el feo y el malo.** **RAÚL SILES, Founder & Senior Security Analyst, DinoSec.**
17.00 HS	**CLAUSURA**

Sigue el encuentro en **Twitter** con los hashstags **#CyberSecurity** y **#4ForoCSC**

EN UN MUNDO FASTER FORWARD

Los ataques cambian, pero nuestra habilidad para detenerlos no.

Es un hecho. Los ataques cada vez son mayores, más potentes y más frecuentes. Y, desafortunadamente, casi cualquier organización que tenga presencia online puede ser su objetivo. Con Akamai, no hay necesidad de poner en riesgo los ingresos, la reputación de nuestra marca o el servicio al cliente por causa de un ataque a la infraestructura o a nivel de aplicación. Creemos que una defensa proactiva es el mejor ataque contra actores maliciosos.

akamai.es/seguridad

Akamai

DECONSTRUCCIÓN Y ANÁLISIS DE UN ATAQUE DDOS

Federico Dios, Service Line Manager Akamai Technologies.

La amenaza que plantean los ataques DDoS (Denegación de Servicio Distribuido) y a aplicaciones web sigue creciendo trimestre tras trimestre como así lo detalla el último Informe de Seguridad del Estado de Internet del Segundo Trimestre de 2015 de Akamai. El informe, que ofrece un análisis y visión sobre el panorama global de amenazas de ataques a la seguridad de la nube (www.stateoftheinternet.com/security-report), confirma que la actividad de ataques DDoS ha establecido un nuevo récord en el segundo trimestre de 2015, incrementándose un 132 % en comparación con el segundo trimestre de 2014 y un 7 % en comparación con el primer trimestre de 2015.

Cuanto más se sabe sobre amenazas de ciberseguridad, mejor se puede defender una organización, y conocer en profundidad cómo funciona un ataque DDoS, es crucial para estar preparado y defender la seguridad de cualquier tipo de empresa de ataques que se duplican año tras año aunque las tendencias varíen. Nuestro último informe apunta que los atacantes prefirieron ataques menos potentes pero de mayor duración y que se produjeron 12 ataques con picos de más de 100 Gigabits (Gbps) y cinco ataques con picos de más de 50 millones de paquetes por segundo (Mbps). Muy pocas organizaciones tienen la capacidad de soportar, por si mismas, este tipo de ataques.

Federico Dios, Service Line Manager de Akamai Technologies analiza paso a paso en su ponencia del IV Foro de la Ciberseguridad del Cyber Security Center, cómo se desarrollan los ataques DDoS más recientes, tipo DD4BC y XOR, desde su planteamiento inicial, donde se detectan los primeros síntomas de infección binaria. Durante su intervención, descomprondrá la actividad maliciosa atendiendo al número de ataques, la media de ancho de banda pico y la media de paquetes pico por segundo. Asímismo, individualizará la intervención maliciosa por países e industrias y finalizará con recomendaciones prácticas de medidas posibles a aplicar para la detención de este tipo de malware.


BLUE COAT
Prepare.
Proteja.
Detecte.
Responda.
Construya una estrategia de seguridad capaz de adaptarse a las nuevas amenazas avanzadas con las soluciones **Advanced Threat Defense** de Blue Coat.
Acceda a nuestra guía interactiva para saber más:
bluecoat.com/atd-guide

BLUE COAT

EL "BACK DOOR" UNIVERSAL

Alberto Cita, SE Manager, Southern Europe, Blue Coat.

Los ciberdelicuentes han descubierto que la publicidad web puede usarse de una forma muy efectiva para distribuir malware usando Exploit Kits.

Esta técnica de distribución de malware se conoce como Malvertising, y combina de una forma única publicidad web con los Exploit Kits.

Gracias a la publicidad web, desde el punto de vista de los ciberdelincuentes, todos los websites del mundo tienen ya un "back door" incorporado: los web ads contienen código (javascript generalmente) que se ejecuta en casi cualquier sitio web sin conocimiento del propietario del sitio, generando además más tráfico hacia el Exploit Kit de lo que los cirberdelincuentes hubieran podido llegar a soñar usando otras técnicas.

Añadan a la ecuación la visibilidad y el control que proporcionan las redes de publicidad, tanto para los usuarios legítimos como para los fraudulentos, y obtienen el método de distribución de malware con mayor ROI que existe hoy día.

En esta presentación vamos a presentar un informe de Blue Coat Labs que aborda en detalle:

- Las técnicas de Malvertising
- Sus principios de funcionamiento
- Las razones de su efectividad como mecanismos de distribución de malware
- Su prevalencia frente a otras técnicas maliciosas
- Las razones de su efectividad
- Los principales actores

Como final de la sesión se presentarán algunas recomendaciones en cuanto a mecanismos de defensa y unas previsiones futuras de este fenómeno.

Deloitte.

EL RETO DE CONSTRUIR Y MANTENER DISPOSITIVOS IOT SEGUROS

El Internet de las cosas es una realidad a día de hoy. Vehículos conectados, casas domóticas, edificios y ciudades inteligentes, wearables como los smartwatches, y todos ellos con una dirección IP e intercambiando datos por Internet. No obstante, queda todavía mucho camino por recorrer y en la actualidad únicamente el 1% de las "cosas" en el mundo físico tiene conexión a Internet, lo que se estima de forma cuantitativa en 5 millones de dispositivos. Para el año 2020, se prevé que el número de dispositivos conectados a Internet aumente significativamente, pudiendo alcanzarse la cifra de 50.000 millones de dispositivos.

La creciente preocupación por la ciberseguridad en sector de las TIC tradicional es aún mayor, si cabe, en el Internet de las cosas. Esto se debe principalmente a dos razones, la primera es que este tipo de dispositivos interactúan con el mundo físico, y por lo tanto, un ciberataque en este ámbito podría acarrear consecuencias directas sobre las personas. La segunda preocupación, son las limitaciones que existen con respecto a la capacidades de gestión de la ciberseguridad en estos entornos más limitados en recursos.

La industria de las TIC ha reaccionado en los últimos años mejorando todo el ciclo de vida de sus productos incluyendo aspectos de seguridad en todas y cada de sus fases. Esta buena práctica no está tan arraigada en fabricantes tradicionales de sistemas de control, que, ahora empiezan a incorporar conectividad con Internet a sus equipos.

De este modo hemos asistido recientemente a demostraciones de expertos de ciberseguridad que han conseguido controlar remotamente vehículos. El origen del problema radica en un diseño deficiente del modelo de seguridad empleado en las comunicaciones entre los sistemas embarcados y los servicios remotos. Nos surgen así cuestiones como: ¿Los fabricantes de IoT han identificado todas las nuevas amenazas al conectarlos a Internet?, ¿Qué medidas de protección se emplean? ¿Se hacen pruebas de seguridad de algún tipo?

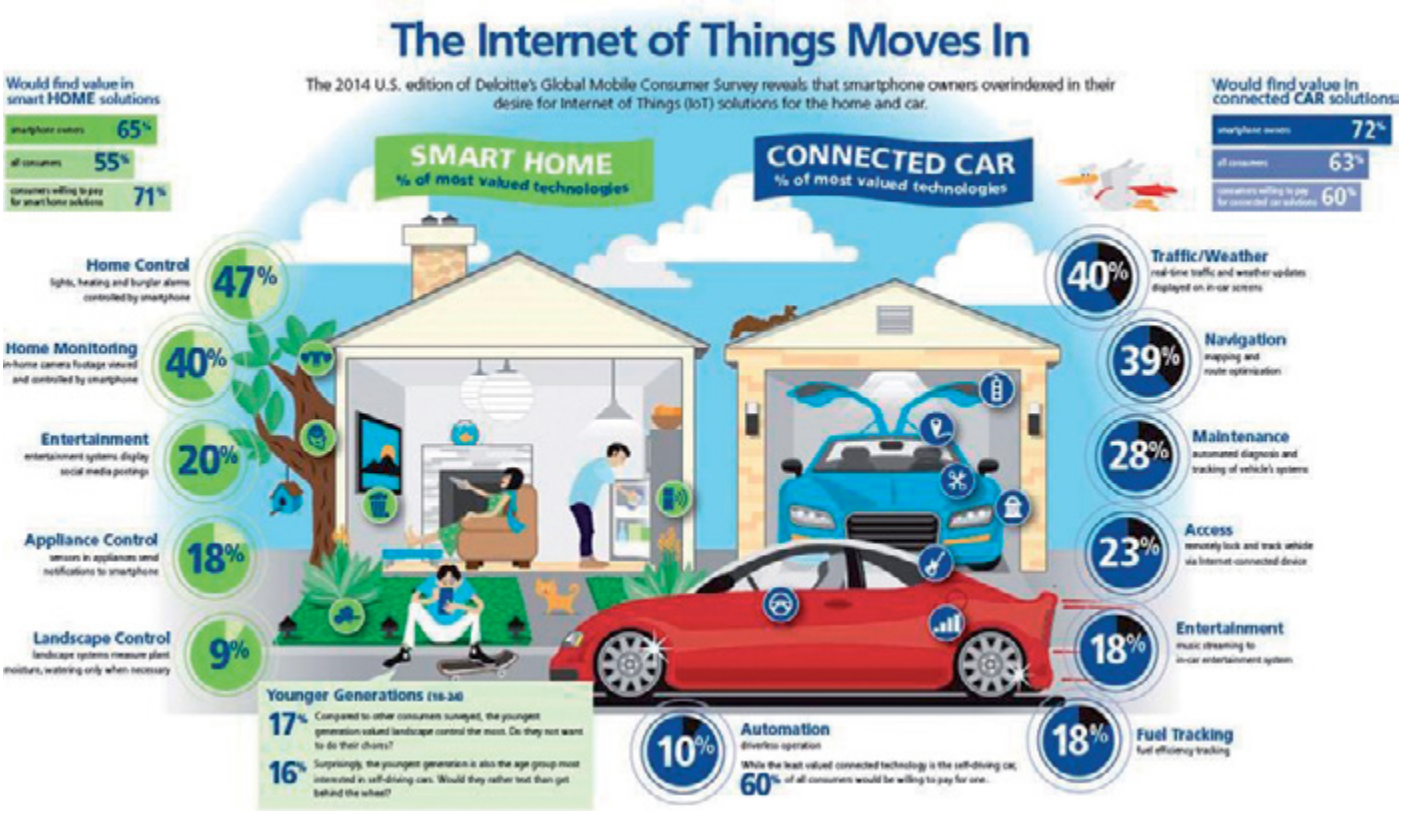
Los sistemas son cada vez más complejos, basados muchas veces en sistemas operativos comerciales, no exentos de fallos de seguridad conocidos. En la informática clásica, su actualización es relativamente sencilla, pero en IoT surgen cuestiones como ¿quién va a actualizar el firmware de los dispositivos sobre los

que el usuario no tiene control?, ¿cómo se van a desplegar estas actualizaciones y de qué forma?

En los sistemas TIC convencionales, gran parte de los problemas de seguridad se resuelven recurriendo a técnicas criptográficas que protegen el software, las comunicaciones y los datos. Estos mecanismos consumen muchos recursos, que, en sistemas IoT, al estar más limitados en hardware, puede suponer un reto su implementación. ¿Cómo se puede alcanzar este compromiso entre seguridad y capacidades del hardware?

Los fabricantes inmersos en este proceso de transformación del IoT deben plantearse incorporar en todo el ciclo de vida de sus productos medidas de protección frente a ciberataques, máxime cuando estos dispositivos pueden manejar información personal como biometría, ubicación, consumo energético, etc.; controlar sistemas que puedan provocar accidentes y causar fatalidades a personas o cuantiosos daños materiales.

Es una excelente oportunidad para que la industria del IoT crezca desde el principio incorporando en su base la seguridad, y que ésta aporte valor a un ecosistema todavía por despegar y tan sensible por sus implicaciones en la salud y el bienestar de las personas.



CIBERSEGURIDAD, PRIORIDAD ESTRATÉGICA EN LA EMPRESA

Emmanuel Roeseler, director de Sistemas de Seguridad de IBM España, Portugal, Grecia e Israel.

Un mundo con mayores posibilidades, más abierto y más innovador como el que posibilita la tecnología es, inevitablemente, un mundo más expuesto al riesgo. Existe una amplia variedad de tipos de peligros en la Red que las empresas no conocen y que les suponen cada año pérdidas millonarias a las mismas, llegando a superar la cifra de 100 millones en la mayoría de los casos. Lo que buscan los ataques fundamentalmente es o bien buscar información o buscar dinero, directa o indirectamente. Y hay una tercera intención que es la de dañar la imagen de la empresa.

La clave no es, evidentemente, quedarse quieto para evitar el peligro. Se trata de avanzar más deprisa y con más inteligencia para ser capaces de responder a los riesgos, asegurándonos de que todo el enorme potencial de innovación y progreso que contiene la sociedad digital pueda desarrollarse plenamente.

En eso trabajan los 6.000 expertos que componen la unidad de Seguridad de IBM, dedicados a dar respuesta a los desafíos de seguridad de los clientes y colaborando con organizaciones e instituciones de todo el mundo.

La visión de IBM en torno a la ciberseguridad se centra fundamentalmente en tres aspectos: la inteligencia: la seguridad no puede estar aislada y tiene que estar muy asociada al negocio. La inteligencia permite saber lo que está pasando en tiempo real en la empresa, tanto dentro como fuera. El segundo es la integración: integramos todas las tecnologías en una solución completa que engloba todo el proceso de adopción de nuevas entornos. Y, por último, es necesario contar con un equipo de gente con experiencia y conocimiento en seguridad; en muchas soluciones de IBM lo que hay detrás es un grupo de expertos que están analizando continuamente lo que está pasando para anticiparse al ataque. Nuestra tecnología estudia el comportamiento de las personas, de las aplicaciones o de las máquinas para minimizar el tiempo que pasa desde que se produce un ataque a la reacción al mismo.

Otro aspecto importante es que, en la lucha contra la ciberdelicuencia, cuanto más reforcemos la colaboración y la unión de experiencias y capacidades entre empresas, instituciones y entidades públicas, mejor preparados estaremos como sociedad

para combatir y superar las amenazas. En este sentido, IBM anunció recientemente que más de 1.000 empresas de 16 industrias están participando ya en su plataforma X -Force Exchange Threat Intelligence. Esta plataforma incluye uno de los más amplios y completos catálogos de vulnerabilidades del mundo: información acerca de amenazas basada en la supervisión de más de 15.000 millones de eventos de seguridad cada día y datos sobre amenazas basados en más de 25.000 millones de páginas web e imágenes.

Tanto para los actuales como para los nuevos retos en materia de seguridad, IBM apuesta por un enfoque integral con su software de seguridad que incorpora seguridad inteligente, analítica y prevención de amenazas externas para ayudar a las empresas a optimizar su estrategia de seguridad, frenar las amenazas más sofisticadas y proteger sus activos críticos. Y con una oferta de servicios que se basan en análisis de comportamiento tanto de dispositivos como de personas incluso fuera del entorno de la propia empresa.

ATAQUES DIRIGIDOS Y ATAQUES DE DÍA CERO

Las últimas estadísticas de seguridad han mostrado que los Ataques Dirigidos y los Ataques de Día Cero se han convertido en una amenaza persistente y silenciosa, tanto para grandes corporaciones como para medianas y pequeñas empresas.

Este nuevo escenario representa todo un reto para las organizaciones, que buscan un nuevo modelo y cultura de seguridad que exige la necesidad de identificar anticipadamente los riesgos. En otras palabras, es necesario evolucionar de la actual cultura reactiva a una de prevención y resiliencia. ¿Cómo?

Convierta su IPS en una herramienta de Protección de Red....

¿Se ha planteado la posibilidad de contar con soluciones que extiendan la capacidad de su IPS aportando visibilidad de los flujos de red aportando una visión horizontal a la visión vertical que tradicionalmente le han ofrecido los sistemas de prevención de intrusiones?

Aproveche los datos del flujo de red para identificar y caracterizar las amenazas más allá del perímetro del sistema de prevención de intrusiones. Sin necesidad de firmas analice comportamientos sospechosos e identifique de forma efectiva las anomalías que van más allá de las capacidades tradicionales de dispositivos basados en firmas.

Añada inspección de contenidos a su arquitectura - Identificación proactiva de malware de Zero Day

¿Se ha planteado añadir inspección de contenidos a la arquitectura de prevención de intrusiones? Aborde los tres requisitos clave necesarios para resolver el problema de las amenazas avanzadas de hoy día: detectar, bloquear y corregir. ¿Cómo? A través de técnicas de Sandboxing, emulación y técnicas globales de reputación generando indicadores de Compromiso basados en estándares y totalmente interoperables.

Análisis en Tiempo Real, desarrollo de la capacidad reactiva y cumplimiento normativo

1.- Desarrollo de la capacidad proactiva en la identificación del malware, recogiendo los eventos generados por las distintas fuentes de información, realizando perfiles estadísticos del tráfico, desarrollando procesos de enriquecimiento de los datos, ofreciendo así, la capacidad de reaccionar sobre la infraestructura desencadenando acciones que desarrollan la estrategia proactiva de la organización en su lucha contra la prevención del malware.

2-. Desarrollo de la capacidad reactiva (resiliencia), ¿Qué ocurre cuando averiguamos que hemos sido víctimas de un ataque Zero Day? ¿Qué otros equipos están infectados?¿Qué información se ha visto comprometida? Recoja Indicadores de Compromiso y desarrolle procesos de correlación histórica, reproduciendo la información de meses sobre reglas de correlación que obedecen a indicadores que se acaban de identificar.

Disponga de un acceso completo y correlacionado a los datos y el contexto necesarios para tomar decisiones rápidas y acertadas.

Añada Indicadores de Compromiso (IoC) a la arquitectura del puesto de trabajo

Añada a la arquitectura de protección del puesto de trabajo la capacidad de utilizar Indicadores de Compromiso (IoC) basados en la reputación del objeto ejecutado en tiempo real, incorporando información de reputación local, Enterprise –contextualizada al entorno de la organización- y global. Proporcionando una respuesta efectiva e inmediata ante nuevos ataques especialmente malware de Zero Day y malware polimórfico a los nuevos ataques.

LA CONTINUIDAD DE NEGOCIO COMO CAMINO INEXORABLE HACIA LA RESILIENCIA ORGANIZACIONAL: ALINEANDO EL MUNDO FÍSICO Y EL MUNDO DIGITAL.

2015: La seguridad corre inexorablemente hacia un lugar desconocido. El mundo, interconectado, no para de cambiar. El conocimiento se distribuye eficientemente y potencia la innovación, desencadenando nuevas amenazas para la sociedad.

Seguridad Física, Seguridad Informática, Seguridad de la Información, Ciberseguridad,...

Según el informe "Horizon Scan 2014 del Business Continuity Institute (BCI)", la amenaza que más preocupa es la de ciberataque. En el estudio realizado por el CSC del ISMS Fórum, la amenaza que más preocupa a las empresas españolas es Indisponibilidad no planificada de IT y Comunicaciones.

Estos informes, entre otros, reflejan la necesidad por parte de las empresas de disponer de mecanismos claros y definidos que cubran las expectativas de protección de la sociedad.

Se está desarrollando la "ISO 22316 Societal security – Organisational Resilience" que define la resiliencia como la agilidad y capacidad de adaptarse a circunstancias cambiantes y convertirlas en oportunidades sostenibles de forma inmediata o a largo plazo. Por otro lado, podemos definir la resiliencia organizacional como la capacidad de adaptación para anticiparse y gestionar un evento disruptivo en todas sus formas, buscando minimizar el daño a las organizaciones y maximizar cualquier beneficio asociado.

El trasfondo de la gestión de riesgos es ver las amenazas del pasado e imaginar las del futuro, mientras que el trasfondo de la continuidad de negocio es mantener al cliente siempre satisfecho. Sin embargo, la premisa de la resiliencia organizacional es integrar disciplinas preventivas, las cuales son esenciales para la ésta, como: la cultura, la gestión de crisis, la gestión de la continuidad de negocio, la gestión de riesgos, la ciberseguridad, la gestión de cambios y el horizon scanning.

Teniendo en cuenta que nuestra sociedad está sustentada por sistemas dinámicos y complejos, uno de los retos actuales es construir una imagen coherente de las

amenazas que podrían estar frente a nosotros. En un contexto de cambios exponenciales y acelerados tenemos que buscar estrategias para anticiparnos a lo que puede suceder en el futuro. En su defecto, las sorpresas crecerán y generarán incertidumbre en nuestro entorno.

Un primer paso para recorrer este nuevo camino puede ser alinear la continuidad de negocio con la ciberseguridad. La forma más práctica y eficiente es prepararnos para un ciberataque extendiendo la Gestión de Crisis a la alta dirección. Cuanto más preparada esté la alta dirección para reaccionar a un ciberataque en términos de precisión y premura, más influirá en una reducción del impacto en el negocio.

A nivel práctico, es necesario incluir en la continuidad de negocio el riesgo de ciberataque, de forma que nos permita implementar un nuevo escenario de continuidad de ciberataque. Este escenario deberá ser probado tanto en su vertiente estratégica (Plan de Gestión de Crisis y Plan de Comunicación) como en su vertiente más táctica (Planes de Recuperación), ligada a aspectos operativos. Es vital que todos los involucrados conozcan sus responsabilidades en situación de crisis y que hayan practicado las funciones a desarrollar, permitiendo a la organización avanzar hacia una nueva cultura corporativa basada en la resiliencia organizacional.

CRYPTOLOCKER: LA PASTA O LA INFO!

Carlos Fernández, Cybersecurity Technical Leader, Symantec.

En los últimos tiempos estamos experimentando un auge importante de las amenazas conocidas como troyanos *Ransomcrypt* que cifran el contenido de los mismos, haciendo inaccesible la información hasta que se produzca un pago con el que obtener el método de descifrado.

La amenaza catalogada por Symantec como *Trojan.Cryptolocker*, o simplemente *Cryptolocker*, se ha hecho popular y desgraciadamente famosa. *Trojan.Cryptolocker* cifra ficheros de datos (ofimáticos, imágenes, etc.) residentes en máquinas infectadas y exige el pago de una suma de dinero, con una cuenta atrás, para descifrar los archivos afectados. La gravedad se acentúa si tenemos en cuenta que este troyano no sólo es capaz de cifrar ficheros locales de máquinas infectadas, sino también unidades de red residentes en servidores a las cuales el usuario infectado tiene acceso.

Mientras que en una amenaza de malware tradicional, a los ficheros infectados se les añade código malicioso que puede ser detectado por una firma antimalware, en este tipo de amenazas en cambio los ficheros infectados son cifrados, haciendo poco efectivo este método de detección tradicional.

Esta nueva tipología de amenazas no es eficazmente frenada con los mecanismos tradicionalmente empleados hasta ahora. Si el problema evoluciona, también debe hacerlo la solución. Es frecuente el caso de organizaciones que hacen uso de soluciones antimalware actualizadas y correctamente configuradas que, si embargo, se ven afectadas por amenazas de este tipo, lo que acentúa más si cabe **la necesidad de redefinir las estrategias de protección** y abordar las nuevas amenazas desde otras ópticas.

¿Cómo minimizar riesgos?

Las medidas de protección básicas existentes (típicamente soluciones antimalware) deben ser complementadas con soluciones de protección avanzada que nos protejan incluso ante lo desconocido. **Symantec Critical System Protection** y **Symantec Datacenter Security**: **Advanced** aportan una visión diferente a la protección de sistemas. En lugar de comparar con algo previamente conocido y

malicioso, permiten **definir de forma precisa qué puede ejecutarse en un sistema y con qué niveles de privilegios.**

Cryptolocker emplea su propio binario para llevar a cabo los cifrados. Si ese binario es "contenido" en un área del sistema a la que enviamos todo lo no permitido, definiendo unos privilegios mínimos sobre la misma, podemos, en última instancia (y si todos los niveles de control anteriores no han funcionado como se esperaba) no evitar que Cryptolocker llegue a un sistema final, pero sí *evitar que actúe. Es decir, el proceso que el malware intenta lanzar sobre ficheros locales y de red no tendría acceso a su objetivo, y por lo tanto no podría cifrar los archivos finales.*

Adicionalmente **Symantec Critical System Protection y Symantec Datacenter Security: Advanced** permiten definir procesos y usuarios para el acceso a la información, efectuar virtual patching, detener el escalado de privilegios y efectuar bloqueos de tipo "Buffer Overflow".

Para una información más detallada puede ampliar esta información con su representante comercial de Symantec o en http://www.symantec.com/data-center-security/

VISIÓN DE UN MALWARE BANCARIO ACTIVO

Renaud Bidou, director técnico para el sur de Europa.

Pkybot (aka Tbag) es un malware bancario reciente, comenzó a operar a principios de julio y todavía se mantiene muy activo. Al analizarlo, revela las técnicas actuales utilizadas para el comprometer, evitar, infectar y controlar. También ofrece la oportunidad de profundizar en las tecnologías subyacentes de uso común, como el cifrado ligero, los kits de exploits y WebInjections.

Pkybot es una evolución de Bubilk, que se ha enriquecido con nuevas técnicas de propagación como el uso de Nuclear Exploit Kit lanzado desde sitios web comprometidos. La estructura de este exploit es un conjunto de herramientas en evolución dirigidas a navegadores web aprovechando vulnerabilidades recientes que, en su mayoría, se encuentran en plugins. También es capaz de detectar los anti-virus con el fin de evitar ser descubierto... A partir de este punto el malware se descarga y se inicia el proceso de infección.

La primera fase se centra en establecer una conexión entre el equipo comprometido y un servidor de Comando y Control (C2). Esta conexión está cifrada y utiliza un mecanismo asimétrico con una clave proporcionada por el servidor C2, una vez establecida la comunicación.

A continuación se indican varias operaciones típicas de malwares bancarios:

- Recopilación de información del sistema
- Actualizaciones de Pkybot
- WebInjection
- Man-in-the-Browser a través de DLL o EXE

El primero y el segundo se utilizan para mantener una lista actualizada de los sistemas comprometidos y adaptar los vectores de infección a posibles correcciones.

Los 2 últimos son los más interesantes, ya que apuntan a la manipulación de datos directamente desde el navegador, lo que sin ninguna duda significa cifrado (SSL). También VirusTotal alcanzó, dos meses después del lanzamiento del malware, variaciones de entre 2/56 y 4/56, dejando la carga maliciosa prácticamente indetectable una vez descargada y ejecutada en el equipo comprometido.

En esta etapa todas las transacciones web están comprometidas: los datos son robados o manipulados, los usuarios son redirigidos de forma transparente a sitios de phishing, los enlaces maliciosos insertados en aplicaciones móviles falsas, etc.

Sin embargo, los hackers cometieron un error en la actualización de los servidores C2 que se proporcionaron al host del equipo comprometido a principios de agosto: señalaron a algunos nombres de dominio no registrados. Un equipo de investigadores ha registrado los dominios y ha configurado un área para recopilar todas las comunicaciones entre los hosts comprometidos y su servidor C2 falso.

Esto ha hecho posible el análisis de una muestra de la infección global y observar la propagación geográfica del malware, así como los objetivos del proceso de WebInjection. Curiosamente, los atacantes parecen ser muy conscientes de la situación y contexto económico de sus objetivos. En efecto, mientras que en la primera etapa de la infección la mayoría de los bancos a los que se dirigieron eran griegos, el enfoque cambió por completo a principios de agosto para apuntar a los españoles...

Después de esta experiencia, se deben aprender varias lecciones sobre el ciclo de vida del malware y su capacidad de adaptación al contexto técnico y económico, la reutilización de las variantes de códigos maliciosos de terceros, la evolución de la estructura de las redes de comando y control de botnets y los errores de los atacantes hacen que se pueda utilizar para el contraataque...

Sin embargo el botnet sigue vivo y la puntuación VirusTotal de Pkybot sigue siendo relativamente baja en 34/57.

Una iniciativa de :

isms forum spain

CSC Cyber Security Center

PATROCINAN:

Akamai

BLUE COAT

Deloitte.

intel Security

IBM

NECSIA

SAMSUNG

Symantec.

TREND MICRO

COLABORAN:

Obra Social "la Caixa"

apd Asociación para el PROGRESO de la DIRECCIÓN el saber conecta

Paseo de la Habana, 54,
2º Izquierda 1.
28036 Madrid - España
Tlf :+34 91 563 50 62

+info:
info@ismsforum.es
www.ismsforum.es

@ISMSForumSpain