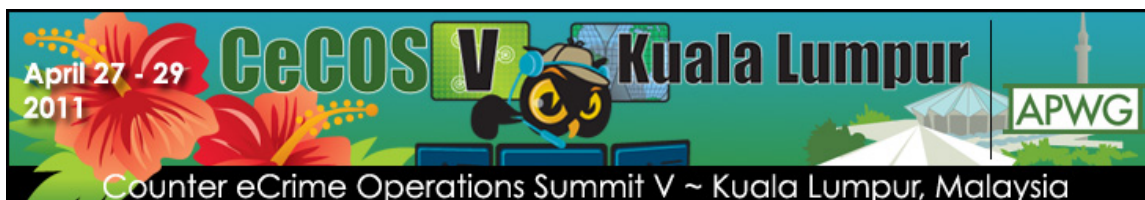


INFORME: EVENTO DE SEGURIDAD INFORMÁTICA – SEGURIDAD DE LA INFORMACIÓN – CECOS V – APWG (Anti-Phishing Working Group)



RESUMEN COMPLETO DE LAS PRESENTACIONES

El **Malaysian Computer Emergency Response Team (MyCERT)**, ha desarrollado Cyber999, que es un servicio que actúa vía E-mail, SMS y novedosamente como un add-on (complemento o extensión) para navegadores Firefox y Chrome, con el cual, cualquier usuario común denuncia y reporta ataques de phishing, hacking e incidentes, ante este centro nacional de emergencias.

Japón, a través del **HitachiJoho** y del **Council of AntiPhishing**, ha logrado reducir el SPAM, de 55 billones de envíos diarios a casi 33 billones. Esto se debió al desmantelamiento de la red botnet "Rustok", conocida por ser la red de computadoras con mayor envío de spam a nivel mundial. Ahora, el 75% de los celulares allí sufren el SPAM.

Las fuerzas de justicia de Japón, en enero este año, arrestaron a 7 ciberdelinquentes que enviaron 5 millones por vez, de SPAM por SMS desde computadoras distribuidas en China, Filipinas y otros países asiáticos. Esta banda, en poco más de un año, había recaudado 5 millones de dólares.

El **Grupo-IB de Rusia**, aportó datos y cifras sobre los principales problemas que les afectan: phishing en productos por Internet, sitios de bancos y tarjetas de crédito.

En el mundo, en ataques desde computadoras se perdieron 7 billones de dólares.

En Rusia de ese monto, se acusaron 2.5 billones.

El ciberdelito gana allí más de 1.3 billones.

El fraude en homebanking es de más de 26 millones por mes.

El costo de servicios y productos es:

Un programador de virus, cobra por ello entre 900 y 5.000 dólares

El número de una tarjeta de crédito con el PIN vale 500 dólares.

La información de una cuenta o transacción bancaria de 80 a 300 dólares.

El número solo de la tarjeta de crédito, de 5 a 25 dólares.

Un usuario para pagos por Internet (Ej. PayPal), 5 dólares.

Un pasaporte o licencia de conducir falso, 150 dólares.

El **Centro de Investigaciones y Prevención de Delitos Informáticos**, con sede en la **India**, dio a conocer los grandes problemas para la zona que ellos controlan:

Bhután, Sri Lanka, Maldivias y Afganistán, no cuentan a la fecha con leyes para proteger a los ciudadanos y penar a quien cometen ciberdelitos.

India a partir del año 2000 y Pakistán, Nepal, Bangladesh a partir del 2007 implementaron leyes contra el cibercrimen.

Los principales problemas (y en gran cantidad) a que se enfrentan estos países son: Hacking a sitios de Gobierno, de Defensa y Corporaciones.

Robo de documentación confidencial y de correos electrónicos.

Terrorismo por E-mail y Cyber Terrorismo en todas sus formas.

Difamación y acoso a través de las redes sociales o pornografía.

Phishing, hacking de todo tipo de Websites, introducción de virus y malware.

Robo y cracking (romper) de contraseñas, grandes ataques de denegación de servicios a servidores.

Con todas estas armas, los ciberdelincuentes obtienen:

Malversación de fondos, robo y chantaje.

Acoso, acecho y hostigamiento a través de redes sociales, E-mail y teléfonos inteligentes

Adueñarse de todo tipo de cuentas (E-mail, tarjetas, sitios Web, etc.).

Técnicas de phishing para defraudaciones. Supresión, corrupción y robo de datos.

Espiar a Soberanos, ciudadanos y agentes de negocio.

Son creadores o "fabrica" de SPAM y Malware.

Cada una de estas naciones tienen además sus contextos políticos con sus dificultades bien marcadas, entre ellos:

India, con terrorismo de maoístas y la zona estratégica de Cachemira, debilidad en el gobierno y corrupción.

Pakistán y Afganistán, con el desorden interno que provocan Al-Quida y Talibanes.

Precisamente, en toda la región, Al-Quida y los Talibanes desarrollan todas las capacidades del Ciberterrorismo.

Los terroristas son los principales compradores al exterior de Ciberterrorismo y los hackers están activos principalmente en India, Pakistán y Bangladesh.

Generalmente los ataques que se producen son a sitios de Bancos, el Centro Financiero en Bombay, a empresas de tecnología en donde infectan y cierran sus portales hasta por 3 días, además de sitios de compras on-line.

Los ataques que han sido reportados en estos lugares fueron:

La operación china GhostNet que es el nombre a una gran operación de espionaje electrónico donde fueron comprometidos sistemas de computadoras pertenecientes a embajadas y otras oficinas gubernamentales, así como también centros de exilio del tibetano Dalai Lama en la India.

Los servidores de E-mail del Primer Ministro también fueron intervenidos por chinos.

Las passwords de los diplomáticos indios en misiones de gobierno.

A partir de todos estos casos, las leyes en India definen lo que es Cyber Terrorismo, Cyber Café, Intermediarios entre estos y Cyber Seguridad. Penaliza lo que es acceso indebido a confidencialidad y privacidad de datos; interceptación y bloqueo; retención y preservación del tráfico por parte de intermediarios; le otorga a la policía más poder para la búsqueda y la toma o decomiso de evidencia e información.

En Pakistán son blancos preferidos, los Bancos y cajeros automáticos y el sitio oficial del Presidente. Además, el juego on-line, el lavado de dinero y la venta ilegal de productos. Ciberterrorismo, robo de datos, el acoso, difamación y amenazas vía Web; la piratería y el robo de propiedad intelectual y ataques de denegación de servicio en servidores, malware y más.

Pakistán típico 17 definiciones para Cibercrimen, entre las que se encuentran acoso vía Internet, ciberterrorismo, abuso en los sistemas electrónicos, hacking a sitios Web y falsificación con/de medios electrónicos.

Como condena, proponen pena de muerte para el acceso a la seguridad de datos y a causas relacionadas con el ciberterrorismo. Para los demás delitos, condenas a 7 o más años de cárcel.

Como caso especial, podemos citar la ciberguerra declarada entre India y Pakistán, en los 2 últimos meses del año 2010.

ICA (Indian Cyber Army) hackeo y defaceó (modificación de una página Web) 870 Websites de Pakistán, incluidos 34 sitios de gobierno.

PCA (Pakistani Cyber Army) hackeo y defaceó 270 Websites de la India.

Finalmente, todo terminó con una tregua, por el momento.

En Bangladesh, las leyes permiten encarcelar por más de 10 años, a quienes realicen hacking sobre computadoras, quienes suban información falsa o difamatoria o material indecente a la Web.

El **ThaiCERT** de **Thailandia**, tiene bastante bien controlado todos los abusos que se realizan a través de Internet, los números estadísticos que se reportan son realmente bajos con respecto a los demás países. Para ellos, el total de incidentes se divide en SPAM 50%, Malware 15%, Pishing 14% y Escaneo de Puertos + otros, el 21% restante.

La forma de reducir considerablemente el Pishing, fue como consecuencia de concientizar al ciudadano tailandés en ignorar y no responder todo E-mail escrito en idioma inglés, además de no confiar en realizar transacciones a través de Internet.

Luego, tienen los problemas comunes de todo el mundo, principalmente con Facebook, con lo que es la violación de la privacidad, el descrédito y rumores falsos principalmente hacia políticos, la subida de fotos comprometedoras y la falsificación de identidad.

Con respecto a Wikileaks, el gobierno tailandés bloqueó sus contenidos.

Sobre los dispositivos móviles, ponen el foco de atención en la gran cantidad de ellos y su igualdad de poder con las computadoras, por lo cual registran incidentes en Blackberry, Nokia, Android, iPhone, iPad y/o iPod con descargas de malware (troyanos), bluetooth, pishing a través de las APP (aplicaciones) de Bancos y el avance del SPIN o SPam en Mensajería Instantánea.

Las estadísticas **Global Pishing Report** presentadas por **Afilias** e **InternetIdentity**, demuestran que a principios de 2011 existen 205.715.855 nombres de dominio.

De todos los ataques de Pishing registrados en el mundo, el 20 % correspondió a China.

Del total de ataques realizados a sitios Web de China en el 2do cuatrimestre de 2010, el 74% correspondió al sitio Taobao.com, que es el mercadolibre de los chinos.

Pocos sitios son atacados desde sitios .cn (china), la mayoría de los hackers aprovechan sitios de dominio gratis como .cc.co de Korea.

Entre los dominios de nivel superior (ccTLD) con más promedio de tiempo de Pishing se encuentran .cc (Islas Cocos - Australia), .tk (Tokelau – Nueva Zelanda), .br (Brasil), .uk (Reino Unido), .ru (Rusia), y .fr (Francia).

Entre los dominios de primer nivel genérico (gTLD) con más promedio de tiempo de Pishing se encuentran .com, .net, .org, .info y .biz (business).

En este período se registraron 2.066 sitios falsos o con contenido malicioso para el juego WarCraft de Battle.net.

Expertos de los **Laboratorios Kaspersky** de **Japón**, expusieron sobre los principales ataques que debe resolver su antivirus.

Archivos atacados en E-mails.

Ejemplo: archivos estándares y conocidos a los que les cambian una letra o símbolo y en realidad son virus, malware, etc.; como iexplore.exe (navegador) y sus falsos explorer.exe o i-explore.exe o explorer.exe y más.

Descargas de archivos de Internet.

Ejemplo: generalmente al ver o bajar videos, fotos o música. Si voy a ver o bajar un video como http://www.youtube.com/user/sosita_golazo.avi nunca tendría que ser http://www.youtube.com/user/sosita_golazo.avi/archivo.exe, como vemos con .exe final.

Sitios Web comprometidos por el SPAM.

Ejemplo, los acortadores de URL, que te envían hacia otro sitio Web, sitios de productos de farmacia, ver fotos (la muerte de Bin Laden), noticias falsas (terremoto de Japón informando falsamente).

Envenenamiento (imitación falsa) de imágenes en búsquedas con Google Image.

Ejemplo, falsas imágenes de personas populares o sitios de interés, que al hacer click nos redirigen hacia sitios fraudulentos.

Descargas de complementos y utilitarios para sonido, imagen, etc. (PDF, Flash, etc.).
También entran en esta categoría los falsos antivirus, firewalls, actualizaciones, etc.

Los **Laboratorios F-Secure**, dieron su presentación acerca de los ataques que se producen a los smartphones (teléfonos inteligentes).

Zeus, troyano que tanto daño ha causado a los usuarios de banca online y su variante para smartphones Zitmo (Zeus In The Mobile) en referencia al tipo de ataque 'Man in the Middle' o de persona que esta interceptando una comunicación. Los usuarios que inadvertidamente ejecutan este troyano, haciendo click en un vínculo aparentemente confiable. Cuando un cliente de Banco abre un homebanking e inicia la sesión, el troyano captura la información introducida. El troyano puede distorsionar la página Web de un sitio de confianza para capturar la información confidencial. Todo esto en PC's, Notebook o Smartphones. Generalmente los fondos "robados" son transferidos a cuentas de "mulas" de dinero ilegal.

Básicamente, Zeus/Zitmo detecta el nombre de usuario y la clave del cliente en su PC o dispositivo; el Troyano toma el número de teléfono del usuario a través de un formulario malicioso introducido en el navegador del usuario. Envía un SMS, ofreciendo un link a una "certificación" pidiendo que sea instalada. Este paquete descargable contiene a Zitmo.

Una vez realizada la instalación, los cibercriminales, que controlan el Troyano Zeus, pueden iniciar transferencias desde la cuenta de homebanking del usuario y confirmarlas interceptando los SMSs que el banco envía al móvil del usuario.

El precio de este troyano es de 4.000 u\$s y viene con distintos módulos. Se le puede agregar keyloggers (o detector de pulsación de teclado), configuración de archivos encriptados, etc.

Las "mulas" que realizan las transferencias se quedan con el 8-10% de la suma, en Argentina con el 20%.

Hay móviles y sistemas operativos que son más débiles para resistir estos ataques, como el Nokia 5130 XpressMusic. También se instalan a través de las APP de symbian (Nokia, Sony Ericsson, Samsung, Siemens, etc.) o aplicaciones .jar para Blackberry.

Los nuevos ataques toman el IMEI (código que identifica al aparato unívocamente a nivel mundial, y es transmitido por el aparato a la red al conectarse a ésta.) de los teléfonos. Con el control de éste, pueden instalar los programas maliciosos y certificados que quieran, ya que no necesitan confirmaciones, además de controlar los SMS.

En resumen, la base de los ataques se producen sobre las aplicaciones que utilizan los Bancos para utilizar sus servicios.

Trend Micro y AVG Technologies hablaron sobre la importancia de la concientización, la capacitación, las buenas prácticas. Lo importante de realizar mediciones sobre todas las actividades maliciosas y tener siempre presente para contactarse con las agencias y Organismos dedicados a la seguridad informática.

El **Banco de Tokio-Mitsubishi UFJ**, propone incorporar como base de estrategia y documentación la *National Strategy for Trusted Identities in Cyberspace* de los EE.UU. para aplicar entre sus clientes en todo lo relacionado con autenticación de clientes en aplicaciones móviles para Bancos.

El programa busca una solución a los robos de identidad online mediante el cual cada ciudadano debería tener un sistema de identificación, similar al documento o cédula propio que a la vez le daría al gobierno una identidad de cada ciudadano a través de una aplicación y protegerá la información de cada ciudadano en Internet.

Este sistema no necesitaría de contraseñas, sino de un soporte físico individual, una especie de pequeña tarjeta inteligente que, vía smartphone, logrará acceder a datos personales.

Además, desde el Banco de Tokio, proponen mejorar la seguridad de las aplicaciones para smartphones, haciendo aplicaciones más amigables y seguras para el usuario y facilitar el uso de las contraseñas seguras, tratando de eliminar de esta formas las autenticaciones tipo CAPTCHA, biométricos, tokens, certificados digitales, etc.

Ellos también hacen hincapié en que los ataques de basan en tomar el control de los móviles a partir de la descarga de aplicativos, a través de las APP y distintos Stores.

Federal Criminal Police Office de Alemania, narró que allí, en Alemania, los ataques de los hackers apuntan principalmente a los sitios Web de tiendas o compra on-line como t-online.de, 1und1.de, paypal.de y eBay.de principalmente.

También se reportan gran cantidad de ataques tipo Zitmo (Zeus In The Mobile) a teléfonos Nokia N66 entre otros y los problemas de descargas a través de aplicaciones .jar (archivos java), .sis (para sistemas operativos Symbian de algunos móviles Nokia, Sony Ericsson, Samsung) y .cab (archivo comprimido de Microsoft); dependiendo del sistema operativo de cada teléfono.

Suman más problemas, los dispositivos con tecnología y servicio multiSIM que permite tener dos o más tarjetas SIM con el mismo número de teléfono. Así un número de teléfono o tarjeta interceptado por un malware, tendrá el total control de móviles, iPad, iPhone, etc.; y con todos los servicios incluidos de voz y datos, mensajes e Internet.

MyCert (Malaysian Computer Emergency Response Team), de **Malasia**, presentó una solución para Bancos y Corporaciones de la región -CIMBbank, BankIslam, HSBC, AmBank, OCBC Bank y más-, que muchos ya utilizan.

Es un mecanismo de seguridad de prevención para Banca on-line para el Phishing que se instala en el navegador y le avisa instantáneamente al usuario y al Banco ante un intento de descarga de malware, al ingreso a una página Web falsa o ante algún acto de intención de apropiarse de datos personales.

Analiza para todo sitio Web lo símbolos, teclas ingresadas, la procedencia de la dirección Web, pop-ups, adware, otros y en caso de detectar anomalías, inmediatamente despliega un mensaje de sitio peligroso con la opción de reportar el mismo al Centro de Emergencia.

El sitio Web reportado, además es declarado ante el grupo antiphishing.my.

La empresa de Seguridad en Internet **Brand Protect** con sede en **Toronto**, expuso sobre los riesgos en el uso de las redes sociales.

El suceso de estas redes en números y conceptos:

Se envían 6.939 Twitts (Twitter) por segundo en vísperas de año nuevo.

Facebook tiene 3 millones de páginas de clubes de fans.

Cada minuto, se suben a Youtube 35 horas de video.

Las redes sociales son incorporadas a las campañas de marketing.

Los managers de grandes empresas utilizan Blogs para comunicar sus pensamientos.

A través de LinkedIn se incorpora gente a las empresas.

Mediante Twitter se responden las consultas de los clientes.

El riesgo de todos estos servicios son las personas de fines inescrupulosos con actitudes de defraudación de fondos o bienes y de los hackers que roban información personal y crítica de empresas.

La penetración de las redes sociales en el ciudadano, hacen que sea el medio ideal para cometer ilícitos como: pornografía infantil, juegos on-line, fraudes, ciberterrorismo, falsificación y abuso de propiedad intelectual entre muchos actos perjudiciales.

Según sus estadísticas, hay un gran crecimiento en las estafas y cada vez mayor:

u\$s 559 millones en fraude on-line.

u\$s 221 billones en robo de identidad.

u\$s 400 billones por venta de artículos y productos falsificados.

Entre los empleados de Organismos y empresas, el envío de e-mails, publicación de fotos y comentarios subidos a blogs, han sido causa de despidos.

Los falsos perfiles creados en redes sociales, han dejado mal parados a muchas personalidades y a usuarios comunes y, en muchos casos la identidad falsa creada tiene más seguidores que la verdadera.

Por la gran cantidad de usuarios y mensajes que circulan, las redes sociales, son el medio más efectivo para el phishing, el robo de identidad y la descarga de malware.

La solución es actuar con conciencia, capacitarse permanentemente acerca de los riesgos y las nuevas amenazas y utilizar todas las herramientas de gestión de incidentes que se encuentren en el mercado.

Argentina Cibersegura, con Facundo Malaureille (Estudio Jurídico Salvochea) y Federico Pacheco (ESET Latin America), reveló su plan para la región. La “educación” como la gran base para todos los niveles de formación de la población.

Este año han lanzado el portal argentinacibersegura.org con contenidos de enseñanza para todas las edades y para los distintos sitios de utilización como escuelas, Organismos, empresas y hogares, independientemente que sean públicos o privados.

La idea de Argentina Cibersegura esta inspirada en la iniciativa “Securing Our eCity” para “concientizar, educar y actuar”, proyecto surgido en San Diego –EE. UU.-, por ESET North América y el Tour Antivirus de ESET Latin America.

La tarea consiste en capacitaciones permanentes de ciberseguridad a través de charlas, simposios, blogs y eventos por medio de personal de tecnología informática, abogados, y capacitadores experimentados con años de conocimiento en la materia, haciendo énfasis en la utilización de material didáctico en castellano, por ser el idioma predominante en toda la región continental.

Por su parte **Malasia Cibersegura**, se basa en la misma idea sobre la gran importancia de la educación, además de recalcar la diferencia entre la realidad vs. el mundo digital, el sentido común frente a la ignorancia para inculcarlos en el ciudadano hasta llegar a un instinto natural de protección y seguridad. Utilizan colectivos como salón para clases interactivas, con rumbo itinerante.

McAfee Antivirus, bajo el slogan intitulado “Stop.Think.Connect” o “Deténgase.Piense.Conéctese”, lanzó una gran campaña nacional de concientización en EE. UU., sobre los peligros a que se está expuesto al ingresar a Internet, con un gran suceso, ya que desde entonces (octubre 2010) los americanos leen y comprenden las políticas, los derechos y los riesgos de los sitios a los que ingresan.

A partir de este suceso, muchos sitios Web cuelgan de sus sitios el lema “Stop.Think.Connect”, y muchos usuarios agregan dicha leyenda a sus firmas de correo electrónico.

El mensaje hacia los ciudadanos fue el de “responsabilidad personal para la conciencia social”.

Empresas y Organismos tomaron esta campaña para eventos, charlas y la distribución de material educativo en escuelas y entre la gente común.

También se crearon conjuntos de herramientas educativas, sitios Web, mensajes o frases de concientización, se repartieron magazines, publicidad en la calles y hasta se grabó un video para compartir desde la Casa Blanca.

Desmenuzando la frase en palabras, nos queda que:

-*Stop*: antes de usar Internet, tómese el tiempo para comprender los riesgos y aprender a detectar posibles problemas.

-*Think*: dedique un momento para asegurarse de que el camino esté despejado. Busque señales de advertencia y analice de qué manera sus acciones en línea afectarán su propia seguridad y la de su familia.

-*Connect*: disfrute de Internet con mayor confianza, sabiendo que ha tomado las medidas correctas para protegerse a sí mismo y a su computadora.

El sitio oficial es www.stophinkconnect.org

Temasek Polytechnic School of Informatics & IT, con sede en **Singapur**, mostró los beneficios de utilizar SPF (Convenio de Remitentes, del inglés Sender Policy Framework) que es una protección contra la falsificación de direcciones en el envío de correo electrónico. La misma, identifica, a través de los registros de nombres de dominio (DNS), a los servidores de correo SMTP (Simple Mail Transfer Protocol) autorizados para el transporte de los mensajes.

Este convenio puede significar el fin de abusos como el SPAM y otros males del correo electrónico.

Insta a los administradores de servidores de correo electrónico a realizar auditorías periódicas, a utilizar SPF, a tener bien claros la definición de nombres de dominio, de direcciones IPv4 y estudiar bien la transición hacia IPv6.

Sumando a estas recomendaciones, estudiar todos los riesgos a que se esta expuesto durante la administración de servidores y aplicaciones de correo electrónico.

Esta institución propone como ayuda a los administradores, utilizar el siguiente sitio de validación <http://www.kitterman.com/spf/validate.html>.

Trend Micro Inc., habló sobre la importancia de utilizar TDS o Sistemas de Direcciones de Tráfico para detección de fraudes y su seguimiento o investigación.

Separar y entender el distinto tráfico que ocurre entre un usuario y el sitio Web al que se accede, es decir, tráfico de base de datos, filtros, estadísticas, y sitios Web intermedios utilizando TDS.

Con este sistema, se controlan patrones y comportamientos por navegador (IEExplore, Mozilla, Opera), por Sistema Operativo (XP, 7, Mac OS X), por geolocalización, tiempo o referencias y tendencias de búsqueda en google, bing, etc.

Además, reportar y bloquear el uso de IFrames para cometer fraudes en páginas Web.

IFrame, es un elemento HTML que permite insertar o incrustar un documento HTML dentro de un documento HTML principal, en concreto IFrame sirve para crear un espacio dentro de la página Web donde se puede incrustar otra Web y de esta manera realizar phishing, redirigir a un usuario a otros sitios maliciosos, descargar troyanos, etc.

Todo este tema del TDS, utilizado por hackers, agrupa a un conjunto de sitios especializados en realizar estafas. Entre las más comunes encontramos programas falsos, programas pirateados, productos farmacéuticos, pornografía, dating (sitios de citas), casinos y diversos artículos como relojes falsos son la carnada para atraer víctimas y ganar miles de dólares al día.

Partnerka, es el término que adquieren estas redes de afiliados en Rusia especializadas en realizar estafas por Internet con el envío de SPAM, malware y todo tipo de defraudación.

TDS, también es utilizado para ataques tipo "ransomware", que es malware distribuido mediante SPAM y que mediante distintas técnicas imposibilita al dueño de un documento a acceder al mismo. El modo más comúnmente utilizado es cifrar con clave dicho documento y dejar instrucciones al usuario para obtenerla, posterior al pago de un "rescate".

CERT-LEXSI, empresa francesa dedicada al cibercrimen, presentó las técnicas que ellos utilizan para evitar fraudes on-line, la fuga de información y auditorías.

Hablaron como etapa importante la recolección de evidencia en E-mails, nicknames, logs y la búsqueda de datos en grupos como foros y redes sociales.

El perfil de los phishers o personas que van a defraudar por Internet, es generalmente de jóvenes masculinos de entre 17 a 25 años de edad, estudiantes o desempleados y de una misma zona o región de país.

Por ejemplo, los ataques a ciudadanos franceses, se da en un 95% de países del norte de África como Marruecos y Argelia, influenciados por el conocimiento del idioma francés.

Ellos, como empresa consultora y de investigaciones, anuncian que los nuevos blancos preferidos por los atacantes pasarán a ser las empresas de energía, las operadoras de telefonía y los proveedores de Internet.

Google Inc., expuso el avance desde el tiempo pasado de la seguridad hacia las nuevas intervenciones en materia de seguridad de la información.

Google busca siempre proteger al usuario, sus datos privados, sus actividades y le brinda seguridad en todo momento.

Ellos pregonan la idea de unificar la seguridad de los usuarios, tanto en ámbitos públicos como en los privados, además proponen crear y publicar para los servicios de Internet, lo que es en EE UU la National Transportation Safety Board (NTSB) o Junta Nacional de Seguridad del Transporte, que es una agencia federal del Gobierno que se dedica a la investigación de accidentes aéreos y otros significativos del tipo automovilísticos, trenes, marítimos en ese país.

Con toda la evidencia recolectada, determinan las causas y se dedican a publicar recomendaciones de seguridad destinadas a prevenir futuros accidentes.

Telefónica de España, dio su visión de acuerdo a la situación que ellos viven.

Telefónica, cuenta con 3 grandes centros de operaciones: Madrid (España), San Pablo (Brasil) y Lima (Perú), que dan soporte y atención todos sus operadores distribuidos por el mundo.

Al tener presencia global, hablaron de los distintos idiomas, culturas, leyes y efectos impositivos a los que están expuestos a atender para un mismo problema o inconveniente que les surja o para aplicar los mismos procesos diarios operatorios.

O sea, el problema es la diversidad de respuesta ante un mismo inconveniente

Por ser distintas culturas, la variable importancia que tiene el uso de los teléfonos móviles y la seguridad que utilizan, o como medio para estar seguro ante distintas situaciones.

Por ejemplo, se preguntan que sabe y que importancia le da gente al malware en sus móviles, a la pérdida de información importante que almacena en ellos, como fotos o E-mails, a la posibilidad de ser rastreados en sus movimientos.

Cuanta gente piensa en sus móviles al hablar de seguridad personal, como lo es en casos de emergencia, accidente, de robo, para localizar familiares ante distintas circunstancias.

La solución para Telefónica es construir una gran estructura o grupo que involucre personal, dispositivos y procesos.

Aprovechar el potencial de cada una de las tres sedes (Madrid, San Pablo y Lima) y explotarlo en pos de una mejor atención a los clientes distribuidos por todo el mundo, dando respuesta a incidentes desde cualquiera de sus centros, en forma de 24x7x365, valiéndose de la ventaja de las distintas zonas horarias.

Solo dejando fuera de esta estructura global, las oficinas de preventa, venta y atención personalizada in situ.

Hacia el resto de las comunidades de lucha contra el cibercrimen, proponen estandarizar globalmente términos como por ejemplo fishing, pishing, piching, etc. Mencionan la posibilidad de hacer esfuerzos en lanzar estándares únicos de comunicación de incidentes como IODEF (Incident Object Description Exchange Format) que es un modelo de información basado en XML definido por el IETF (Internet Engineering Task Force). IODEF, es un formato diseñado para representar información de seguridad informática a intercambiar entre CSIRTs, siendo su principal objetivo proveer a los grupos de respuesta a incidentes con información normalizada y procesable automáticamente. O, el ASF (ASEAN REGIONAL FORUM- Asociación de Naciones del SurEste de Asia) que lanzó la “Declaración de Cooperación de Lucha contra el Cibercrimen, el Terrorismo y el uso inadecuado del Ciberespacio”.

En resumen, tienen un mensaje como todos, el de formar alianzas y colaborar ante un objetivo común: evitar el fraude.

La **International Islamic University Malaysia**, expuso sobre el crecimiento de ataques informáticos mediante redes Fast-Flux. Esta presentación fue totalmente técnica.

Cada nodo de infección de una red Fast-Flux, toma de 10 a 100 PC como parte del dominio Fast-Flux.

En los últimos tiempos, mediante el uso de esta tecnología, se han logrado ataques exitosos a sitios como Myspace, los servicios on-line de Bancos como Halifax y Barclays de Inglaterra, el famoso malware “Waledac” que infecto más de 1.000.000 de PC’s mediante SPAM, redes botnet como Kraken, Conficker y Torping, además de comprometer a Facebook.

Fast-Flux es utilizada principalmente para sitios de phishing, productos de farmacia, juegos de apuestas on-line, sitios que utilizan las “mulas” en estafas, descargas e infección en navegadores Web.

La técnica que utilizan es mediante servidores que contienen sitios Web ilegales, el envío de phishing a través de e-E-mail para redirigir al usuario al sitio fraudulento y la gran velocidad que tienen para cambiar la dirección IP de los servidores para no ser encontrados.

Los cybercriminales, están adaptando estas nuevas técnicas para mejorar los ataques y aplicarlas a ciberdelitos.

Las distintas variantes de Fast-Flux se clasifican en:

Single Flux: una IP de sitio ilegal que va cambiando rápidamente.

Name Server (NS) Fluxing: una IP de nombre de servidor de DNS que va cambiando continuamente.

Double Flux: una IP de sitio Web comprometido y el nombre de servidor de DNS que va cambiando continuamente.

Hay un término relacionado que es: Domain Flux, caracterizado por cambios constantes en requerimientos a nombres de DNS, configuraciones de dominio DNS que resuelven “todo” lo que este detrás de ellos y algoritmos de generación de dominios.

Para que este tipo de ataque no sea exitoso, ya que son muy difíciles de detectar, hay que tomar ciertas precauciones como ser:

Monitorear permanentemente los cambios en los DNS, detectar anomalías en tiempo real, una clasificación con comportamientos históricos, estudiar detenidamente esta metodología de ataque, mostrar estadísticas y métricas a personal no-técnico. Es conveniente utilizar técnicas de “Datamining” (extracción de datos ocultos o no presentables dentro de los mismos datos) para detectar por ejemplo: la localización geográfica de servidores, cambios en configuración de nombres autoritativos, records A y NS y, el crecimiento de números IP.

Se debe tomar como referencia, el sitio <http://www.dailychanges.com/>; el cual monitorea constantemente todos los nombres DNS para dominios .COM, .NET, .ORG, .INFO, .BIZ, y .US TLDs.

IMPACT (International Multilateral Partnership Against Cyber Threats), con sede en **Malasia**, es de las primeras iniciativas público-privada en contra del ciberterrorismo, y habló sobre Geoexplotación.

La geolocalización es posible gracias a la gran cantidad de dispositivos y aplicaciones que contienen GPS (Sistema de Posicionamiento Global) y su bajo costo.

Cámaras de foto, GPS para automóviles, teléfonos móviles, consolas de juegos, relojes, zapatillas y portales de redes sociales, son algunos de los medios que la implementan.

Con todo esto, toda persona o dispositivo es “encontrable”.

Expusieron sobre cuan confiable es el uso de técnicas de geolocalización, a saber.

Utilizando coordenadas de latitud y longitud agregadas manualmente o digitalmente a un dispositivo de GPS, nos dará la ubicación exacta, NO la real.

El país de locación de un usuario, detectado por dirección IP, es bastante simple y confiable del 95% al 99%.

La ubicación física de un dispositivo es más dificultosa y menos confiable, siempre basados en direcciones IP, del 50% al 80%.

Geopriv WG (**Geographic Location/Privacy**) desarrolla políticas para restringir el uso de la distribución de información sobre localización, motivados entre otras cosas, por el desconocimiento de los usuarios sobre la propia información de localización que difunden sus dispositivos.

Las fuentes de información de localización, a través de GPS, para computadoras puede ser: por dirección IP, dirección MAC, Wi-Fi, infrarrojos, Bluetooth, células GSM/CDMA o ingresadas por un usuario en navegadores Web o Websites.

W3C (World Wide Web Consortium) cumpliendo con su función de crear nuevas tecnologías y realizar recomendaciones para mejorar la Web, lanzó una API (interfaz de programación de aplicaciones) para incluir en los navegadores (FireFox, Chrome, Internet Explorer) y así efectuar geolocalización.

De esta manera, Google Maps con la utilidad “my location” o “mi ubicación”, se vale de esta API para intentar establecer nuestra ubicación. Cuando activamos el servicio, nuestro navegador intenta determinar si hay AP (Access Points) en nuestro alrededor para estimar la ubicación; en caso de no encontrar ninguno, ya sea porque no hay ninguno en nuestro radio o porque nuestra PC no tiene Wi-Fi, la locación se intenta determinar utilizando la IP de la PC, lo que hace que la exactitud se reduzca notablemente.

Quienes nos llevan hacia la geolocalización si no lo controlamos?: los navegadores Web, técnicas de clickjacking (ocultar botones para que al enviar información por Web, en realidad nos redirijan a otro sitio, por ejemplo en Facebook con el botón “me gusta”); teléfonos inteligentes; comprometiendo la seguridad de ruteadores con XSS (Cross Site Scripting), CSRF (Cross-site request forgery o falsificación de petición en sitios cruzados) y DNS Rebinding (un atacante puede sortear firewalls, navegar en intranets corporativas, mostrar documentos sensibles, y comprometer máquinas internas sin parchear o no actualizadas); Access Point de Wi-Fi; fotos, malware y phishing enviados por SPAM.

Atacantes podrían utilizar en forma maliciosa el aplicativo para teléfonos móviles inteligentes “GEOSMS” que hace que un usuario tenga la opción de notificar la localización geográfica con precisión, incorporándolo a un mensaje de texto SMS convencional. Al añadir este dato, el SMS pasa a convertirse en un SMS geoposicionado. Entonces, esta aplicación puede revelar la distancia y dirección a la que se encuentra el remitente respecto al receptor del mensaje o mostrar la ubicación del remitente de forma visual. De igual

forma, es posible etiquetar fotografías con información sobre el lugar exacto en el que se tomó la imagen. Hay servicios que permiten realizar búsquedas de Access Point de Wi-Fi, y ubicar dispositivos y personas a partir de las distancias entre los distintos AP; esto es útil cuando no contamos con un GPS. Por ejemplo: <http://www.skyhookwireless.com/howitworks/coverage.php>, <http://www.shodanhq.com/>.

Por su parte las fotos, tomadas desde cámaras digitales o desde teléfonos inteligentes, contienen información de localización dentro del archivo que la contiene. Estos datos no están visibles, pero existen aplicaciones que leen estos datos ocultos o metadatos (datos que describen otros datos).

A partir de HTML versión 5, que ya incluye una API de Geoposicionamiento en los navegadores, el malware toma un control más eficaz sobre todos los atributos de navegación como JavaScript y distintas instancias de navegación, AJAX (JavaScript para aplicaciones interactivas)

El sitio <http://no-geolocation.blogspot.com>, provee información muy completa sobre como desactivar todos los servicios de geolocalización en navegadores Web, teléfonos inteligentes, aplicaciones como Facebook, Twitter, Gmail, Safari, etc.

Algunas de las recomendaciones que IMPACT comparte son: utilizar software de encriptación; aplicaciones de control sobre geolocalización; no siempre haga click en los sitios u opciones que parecen interesantes; imponer a los distintos fabricantes de aplicaciones que no sea fácil o sin consensuar la disponibilidad de obtener información de localización; etc.; etc.; etc.

La geolocalización es útil cuando: se ha perdido o han robado un dispositivo móvil o una notebook; para ubicar amigos, familiares o en medicina con pacientes médicos y ambulatorios; para notificar el robo de tarjetas de crédito, homebanking, etc.; todo esto siempre y cuando las compañías de servicios respeten la privacidad de los usuarios. Los términos de uso y la información que comparten los usuarios debe ser siempre utilizada con conciencia.

Y en temas de seguridad, es buena esta tecnología cuando se la utilice para contrarrestar a los ciberdelincuentes, para desarrollar proyectos de aplicaciones Web y en honeypot (software o conjunto de computadoras cuya intención es atraer a atacantes, simulando ser sistemas vulnerables o débiles a los ataques) para atraer cibercriminales y poder desbaratar estas bandas de fines maliciosos.

The German Anti Botnet Advisory Center, es el centro de asesoramiento Anti-Botnet de **Alemania**, y que cuenta con el apoyo de la Oficina Federal para la seguridad en las tecnologías de la información (BSI), también alemana.

Recordamos que una "botnet", es un conjunto de computadoras infectadas de forma remota, y tomadas para cometer ilícitos, generalmente con las descargas de "cracks" para activar software sin licencias.

Este Centro, se dedican a atacar a estas redes de botnet, por que:

Hay varios millones de computadoras en el mundo infectadas y que son parte de una botnet.

Alemania se encuentra dentro del TOP10 de países con redes botnet.

Las botnet forman parte de una gran infraestructura organizada para el ciberdelito.

Los principales peligros de dichas redes son: la distribución de SPAM; la descarga de software malicioso; ataques a servidores con denegación de servicios y captura de datos o phishing.

El objetivo de esta empresa es dar soporte a los usuarios en temas de seguridad en Internet; reducir la cantidad de botnets, recuperando los dispositivos infectados (principalmente usuarios de Windows); terminar con las organizaciones cibercriminales y sacar a Alemania del ranking TOP10 de países con actividad maliciosa.

Para realizar estas tareas, trabajan junto a los proveedores de Internet (ISP), y a los vendedores de software antivirus.

Los proveedores de Internet y Bancos, detectan y notifican a los usuarios infectados por botnets y los delegan a este Centro de Asistencia.

Los usuarios llegan a través del sitio <https://www.botfrei.de/>, que se encuentra habilitado también en idioma inglés, español, turco, danés y francés.

Una vez contactados, los usuarios utilizan el software de desinfección DE-Cleaner, para encontrar y desinfectar el software malicioso.

En otro de los apartados del sitio Web, se encuentran las medidas de prevención para los usuarios, entre ellas: chequeos básicos a la computadora; para todos los sistemas operativos y aplicaciones de software que se utilicen, instalar la última versión se service-pack y actualizaciones de seguridad.

Colaboran con esta iniciativa ISPs y empresas que informan en sus páginas Web acerca del proyecto y dan soporte a sus clientes afectados: Deutsche Telekom, Vodafone, Versatel, Avira, Kaspersky, Norton, Symantec, 1und1.de, web.de y gmx.de, entre otros.

Próximamente los servicios financieros como 1822Direkt, Fraspa, Naspa, etc., contarán con este servicio.

Finalmente, presentaron estadísticas de uso de DE-Cleaner anti botnets, entre septiembre de 2010 y marzo de 2011:

Activados por Symantec: 412.571

Activados por Kaspersky (aquí de diciembre 2010 a marzo 2011): 36.188

Activados por Avira (aquí del 1 de marzo 2011 al 31 del mismo mes) 31.455

Total de activaciones = 480.214

Tickets de notificación generados a usuarios: 189.329

De la suma de los totales, menos del 1% de los usuarios necesitó soporte telefónico y la duración de los mismos fue de 18 minutos en promedio.

Larry Bidwell de **IEEE Industry Connections Security Group Executive Committee**, **Pat Cain** de **APWG (Anti-Phishing Working Group)** y **Andrew Cushman** de **Microsoft**, disertaron sobre el proyecto de construir un “modelo de salud pública que de respuesta y manejo sobre el E-crime”.

Hablaron sobre algunos modelos de proyectos que andan dando vuelta en el mundo como:

<http://www.microsoft.com/mscorp/twc/endoendtrust/vision/Internethealth.aspx>,

http://www.guarder.net/eurodig/2011/European_Cybersecurity_Authority_WSProposal.pdf

<http://www.cl.cam.ac.uk/~rnc1/malware.pdf>

Mostraron las similitudes que hay en un plan de salud pública y un plan de salud en Internet:

Educación en riesgos básicos de salud frente a educación en riesgos en el “Cyberspacio”.

Esfuerzos para detectar enfermedades frente a esfuerzos para detectar malware y botnet.

Esfuerzos estadísticos de enfermedades frente a esfuerzos estadísticos del cibercrimen.

Vacunas frente anti-malware y así se podrían seguir nombrando similitudes indefinidamente.

Desde aquí, se podría proponer muchas soluciones como una organización del tipo “guardián de la salud”, metodologías, un vocabulario “común” a todos, compartir conocimientos y demás.

Pero, se necesita de la colaboración de todos, públicos, privados, empresas, organismos, universidades, etc.

Por ejemplo IEEE, es la organización de técnicos más grande del mundo.

Cuenta con más de 360.000 miembros distribuidos entre 160 países, de los cuales más del 45% de esos miembros se encuentran fuera de los EE. UU.

Publican el 30% de la literatura presentada en el mundo referida a temas de Ingeniería Electrónica, Eléctrica y ciencias de la computación.

Anualmente, es sponsor de más de 850 conferencias dictadas alrededor del planeta.

La IEEE Standards Association, está reconocida mundialmente por su cuerpo escrito de más de 900 estándares activos y alrededor de 600 estándares en desarrollo.

El ICSG (Industry Connections Security Group) es un grupo global de entidades de seguridad en computadoras, al que pertenecen otras entidades como:

Malware Working Group (MW), Malware Metadata Exchange Format Working Group

(MMDEF), eCrime Management and Response (Stop eCrime) y Privilege Management Protocols (PMP), cada una de ella atacando el problema desde distintos lados pero siempre para llegar a un fin común; la seguridad de los usuarios.

Para acercar propuestas, se sugiere:

Establecer un vocabulario común y estándar para definir los problemas.

Asociarse con economistas y otras entidades para tratar de entender el “comportamiento irracional” de los usuarios para conseguir más información, a pesar de “ya” haber conseguido demasiado.

Crear y testear nuevas “técnicas de influencias” en usuarios.

Un ranking sobre los niveles de riesgos TOP sería:

Pérdidas Financieras e intercepción de transacciones con transacciones fraudulentas, robo de cuentas de Bancos, homebanking o sitios de pago, actividades de lavado de dinero y extorsión

Perdidas del control de la “red” de trabajo, comprometiendo la seguridad de la misma y produciendo la denegación del servicio.

Malversación de datos privados, de marca registrada o patente y baja en la reputación con actividades como el borrado, modificación o el abuso de datos de las personas y el acoso personal, las amenazas de muerte y más.

Accesos a contenidos restringidos como piratería y pornografía

La distribución de conversaciones privadas y la pérdida de privacidad con la alteración de información personal, la posesión, el tráfico, y la falsificación.

La propuesta de una guía de salud para la población, su interacción y el entorno. Para ello proponen:

Para los usuarios, realizar estudios de cómo son ellos infectados y comprometidos.

Campañas de concientización de las asociaciones por cada región.

En la interacción, utilizar métricas y técnicas de Gap Análisis de como se expande y se extiende todo lo referido a la seguridad.

Intercambio de información

Llevar a cabo investigaciones para determinar la eficacia de los controles en las notificaciones.

Formular y publicar posiciones de cómo deben incrementarse los niveles de transparencia de las personas y dispositivos.

La posibilidad de detener las actividades de eCrime, se debería tratar con:

Documentos y publicaciones formales a través del IEEE.

Conferencias, Eventos, Workshops y demás actividades de capacitación.

Autoridades para matriculaciones.

Compartir bases de conocimiento.

Pat Cain de APWG (Anti-Phishing Working Group), narró en su charla titulada “Standards-based eCrime Reporting”, sobre lo abrumador que es recolectar toda la información acerca de los actos de phishing, procesando y comprobando URLs, etc.; por los distintos formatos a investigar y de cómo se los comunicaban a ellos.

Por ello, el plan que presentan para mejorar, es el siguiente:

Utilizar XML (eXtensible markup language) como formato estándar de datos para IODEF (Incident Object Description and Exchange Format), formato para la descripción e intercambio de objetos de incidentes, para intercambiar información operacional y estadística sobre incidentes.

También, se mostraron algunas desventajas de esta estandarización como por ejemplo no llegar a definir todos los datos que sean necesarios.

Crear las herramientas que la gente necesite y ser “flexible”, dada la evolución diaria del eCrime.

Actualmente se esta tratando de:

Definir esquemas para distintos tipos de datos.

Estandarizar otro tipo de información relevante.

Categorizar los tipos de delitos, riesgos y amenazas.

Concientizar por todos los medios y en todos los ámbitos

Estandarizar definiciones, problemas y soluciones.

Ser multi-idioma, multi-país y multi-sanción.

Canales de comunicación en tiempo real como por ejemplo con jabber (protocolo abierto basado en el estándar XML para el intercambio en tiempo real de mensajes).

Pat Cain, Peter Cassidy, Foy Shiver y Mike D'Ambrogia de APWG (Anti-Phishing Working Group), disertaron sobre “Abusive Domain Name Resolution Suspension Process” o ADNRS.

Este, es un programa que trata sobre los “dominios maliciosos” creados con fines de acciones de phishing, distribución de malware o cualquier otro comportamiento deshonesto. La expulsión para ellos, es quitar la resolución del nombre de dominio dentro de los DNS TLD (nivel superior genérico que ofrece una

clasificación de acuerdo con el sector de la actividad. Por ejemplo .com, .net, .org) por parte del Gobierno, registrado como un comportamiento criminal o de delito.

Pensado para crear relaciones de confianza entre sectores, en donde hoy la confianza es poca o nula. Con roles de usuarios y administradores.

Siendo los beneficios de este programa ADNRS velocidad y escalabilidad, procesos basados en confianza, rastreo o seguimiento y responsabilidades, auditorías, métricas y un porcentaje del 0% -cero por ciento- en falsos positivos.

Algunas de las pistas para encontrar dominios abusivos son:

Los sitios malignos tratan de emular o imitar, generalmente, a sitios de Bancos y financieros famosos.

También, a los dominios nuevos o registrados recientemente.

Utilizan nombre se servidores con muy buena reputación

Los roles dentro del ADNRS serán:

Administrador de inscripciones, Intervenens o entrenadores y registros o secretaría.

Hay equipos de registro, cuya función es la capacidad de juntar varios usuarios para las solicitudes de suspensión.

Por último, y cerrando el evento, disertaron bajo el título “Siglo 21, Aplicaciones de la Ley, Necesidades y Cambios”, **Andre Dornbusch (Bundeskriminalamt Wiesbaden)** de **Alemania**, **Eneng Faridah Iskander (Malaysian Communication and Multimedia Commission)** de **Malasia**, **Toni Felguera (Bdigital)** de **España**, y **Richardus Eko Indrajit (SIRT on Internet Infrastructure)** de **Indonesia**, con **Pat Cain** de **APWG (Anti-Phishing Working Group)** como moderador.

En conjunto se refirieron a que el “gran objetivo” sería investigar incidentes, compartir los datos de los informes, trabajar en conjunto e intentar nuevas alternativas para un mismo propósito: atrapar a los “chicos y chicas (grilz) malos”.

El foco para Internet 2.1 y su evolución hacia Internet 3.0 deberá concentrarse en:

Facebook, el anonimato, los dispositivos móviles, los ataques tipo “Fast-Flux”, las consideraciones hacia la “privacidad” y los temas de arbitraje internacional.

La discusión que se plantea hoy es día pasa por saber:

Cómo van los esfuerzos a las necesidades de nuevas leyes?

Cómo andan los cambios?

Cómo podemos ayudar?

-- FIN --

Autor del Resumen:	Ing. Damián Ienco
Fecha:	2 de Junio de 2011
Nombre del documento:	Evento de Seguridad Informática – Seguridad de la Información – Cecos V – Awg (anti-phishing working group)