Boletín trimestral de RSA FraudAction™

Segundo trimestre de 2015

RSA

EMC²

TENDENCIAS DE TROYANOS

EL PROBLEMA ES EL ARCHIVO ADJUNTO

Desde fines de 2014, cada vez son más las campañas de malware que están incursionando en el reino de los archivos adjuntos de correos electrónicos, utilizando documentos Word y archivos PDF como medio de ataque con macros que descargan los archivos infectados. Recientemente, RSA informó sobre las aplicaciones troyanas incorporadas en documentos Word, disfrazadas como archivos adjuntos PDF y que se implementan no bien la víctima hace clic en el vínculo de archivo incorporado (*ATS_150629 Nueva ola de troyanos en documentos Word*).

Investigando esta tendencia, los analistas de inteligencia de FraudAction descubrieron recientemente una hoja de cálculo de Excel en libre circulación que contiene una serie de supuestas imágenes JPEG como "archivos adjuntos" dentro de la hoja de datos.

La hoja de datos, distribuida como un archivo denominado "chika", al parecer contiene archivos adjuntos e incluye botones de activación para abrirlos. Una vez que se hace clic en uno de los botones, aparece un mensaje que le solicita a la víctima que habilite las macros en Excel. No bien se habilita la macro, se activa la comunicación con un servidor y se descarga el archivo de infección que instala la aplicación troyana Pony Stealer en el equipo de la víctima.

Pony Stealer es una aplicación que roba información programada para robar contraseñas de aplicaciones comunes como las de mensajería instantánea, los clientes FTP, los navegadores de Internet, los clientes de correo electrónico y las claves de CD de Windows. El malware roba todos los conjuntos de credenciales de formularios de envío, incluidos los utilizados en portales de operaciones bancarias en línea, como parte de su robo de datos de rutina. Pony Stealer también actúa como cargador de otros troyanos, descargando e implementando otros elementos de malware como troyanos bancarios para facilitar el robo de credenciales financieras e información de operaciones bancarias en línea. Se suelen encontrar en los mismos servidores C&C en los que está implementada una botnet Zeus.

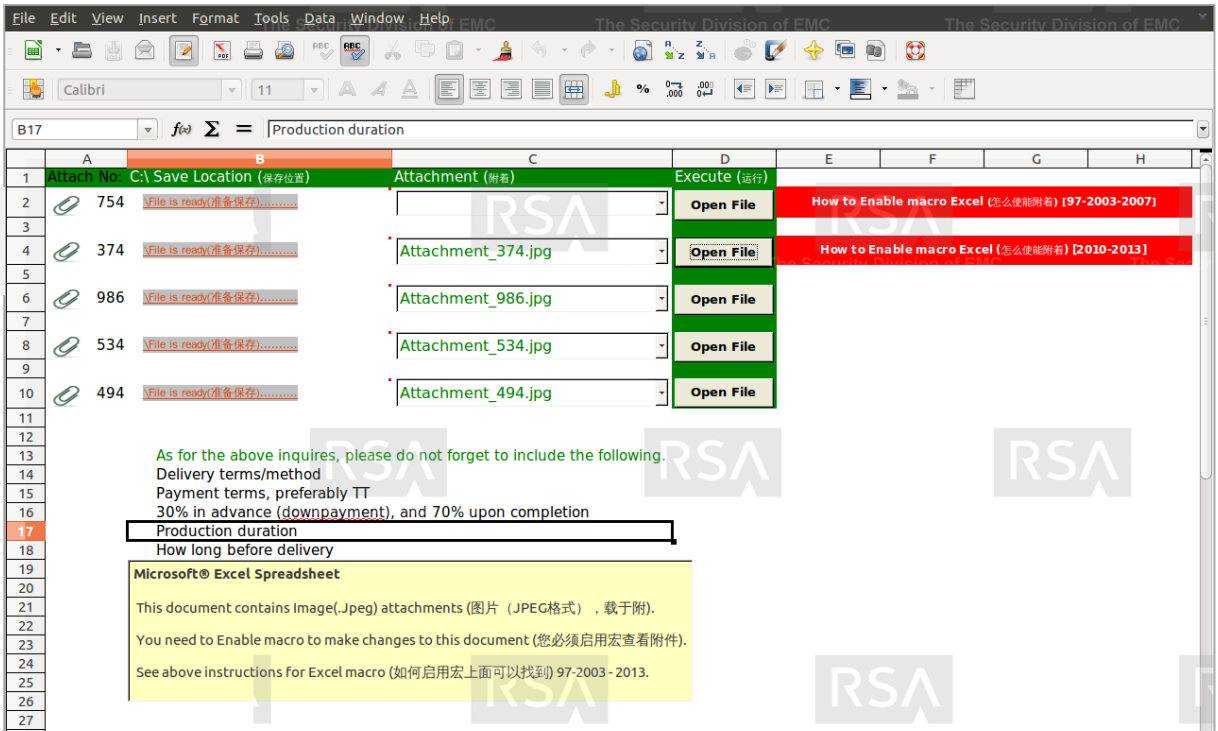


Figura1: Hoja de datos de Excel con archivos adjuntos incorporados

KRONOS SE OFRECE PARA LA VENTA DE MANERA CLANDESTINA

El malware de operaciones bancarias Kronos apareció a la venta a comienzos de julio de 2014, publicitado en un foro clandestino de habla rusa por un precio inicial de US$7000. Kronos (el padre de Zeus en la mitología griega, probablemente una referencia al conocido malware de operaciones bancarias llamado ZeuS) incluye funciones típicas como comunicaciones de servidor cifradas e inyecciones de HTML y JavaScript que se pueden personalizar fácilmente para todos los navegadores web comunes. Las inyecciones web suelen utilizarse para modificar sitios web bancarios legítimos. Una vez que un usuario inicia sesión, las inyecciones web también pueden recopilar información adicional de la víctima, como su PIN de cajero electrónico o información personal útil para responder preguntas de seguridad.

Las funciones adicionales publicitadas del malware incluyen el rootkit Ring3 de 32 y 64 bits (modo de usuario) para ser más sigiloso y defenderse de otros troyanos, omisión de antivirus y omisión de espacios aislados.

Si bien nuestros analistas de inteligencia de FraudAction detectaron una versión en libre circulación en febrero de 2015, el servidor C&C asociado con esa versión ahora está fuera de servicio, y no durante bastante tiempo no se habían detectaron menciones del malware hasta que recientemente rastreamos una nueva noticia en un foro clandestino que ofrece malware Kronos por US$3000. El proveedor solicita que el pago se realice exclusivamente en Bitcoin, y promete que el precio incluye *"una licencia de Kronos de por vida, con actualizaciones, soporte completo y documentación sobre comandos e inyecciones"*.

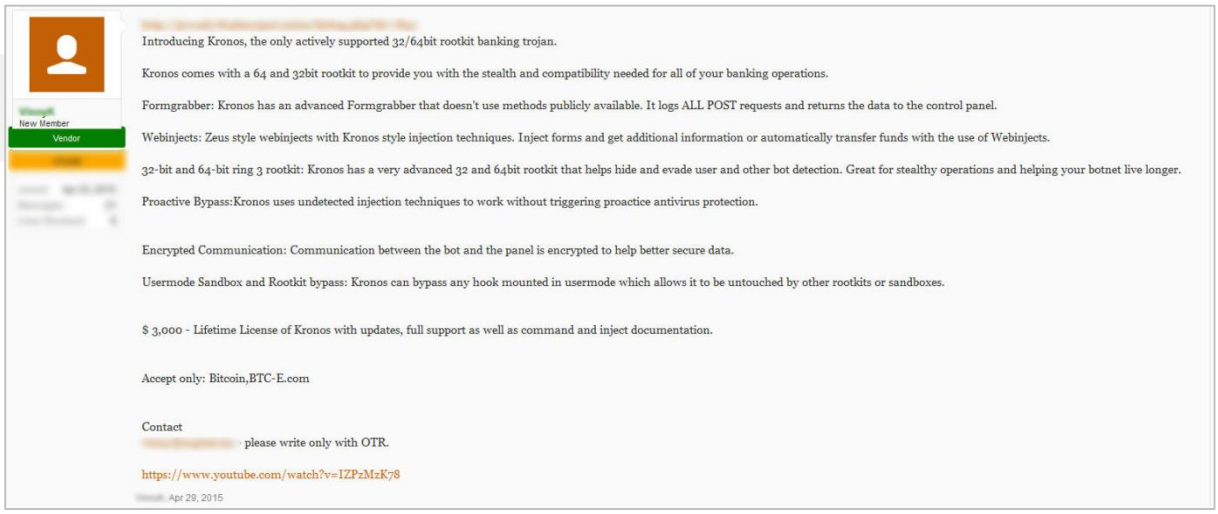


Figura 2: Publicación de foro que publicita la venta del malware Kronos

KITS DE EXPLOTACIÓN

Pese a que los elementos y kits de explotación se encuentran en circulación desde hace ya bastante tiempo, últimamente los suministros de noticias de seguridad de la información han estado informando sobre nuevas instancias que atacan las vulnerabilidades de Adobe Flash Player y, en un caso reciente, se aprovechó la vulnerabilidad para plantar infecciones de malware Ransomware en víctimas desprevenidas.

Un kit de explotación, a veces llamado paquete de explotación, es un kit de herramientas que automatiza el aprovechamiento de vulnerabilidades en el cliente. En otras palabras, estos kits aprovechan vulnerabilidades de las aplicaciones de software de las computadoras de los usuarios finales, generalmente para propagar malware. Los kits de explotación suelen apuntar a navegadores y programas que un sitio web puede invocar mediante un navegador. Entre los objetivos más comunes de los últimos años, se encuentran vulnerabilidades detectadas en Adobe Reader, Java Runtime Environment y Adobe Flash Player.

La mayoría de los proveedores de software distribuyen parches y actualizaciones no bien se detectan nuevas vulnerabilidades, pero depende de los usuarios finales y los administradores del sistema garantizar que se apliquen estas actualizaciones. Según encuestas recientes, al menos un tercio de todas las explotaciones activas en la actualidad se documentaron en 2010, y el hecho de que sigan en uso indica que los usuarios finales no han actualizado el software de la computadora ni aplicado parches que están disponibles desde hace 4 años o más.

Se encuentra disponible una descripción general sobre kits de explotación de puntos vulnerables de 2014 y 2015 en el blog de seguridad Contagiodump.

INVESTIGACIÓN SOBRE LA EXPLOTACIÓN RIG

Un informe reciente de Trend Micro sobre la Evolución de los kits de explotación ubica al kit de explotación RIG en el puesto 4 de los más utilizados en el cibercrimen clandestino, con un 11 % de participación. Los analistas de inteligencia de RSA FraudAction investigaron la reciente filtración del código fuente del paquete de explotación RIG en el entorno clandestino y rastrearon su origen hasta descubrir que el ejecutor de la amenaza era de habla rusa. Nuestros analistas examinaron indicadores como direcciones de correo electrónico (del servicio de mensajería Jabber) e información de registro del dominio Whois, pero no han logrado obtener más información sobre el ejecutor de esta amenaza.

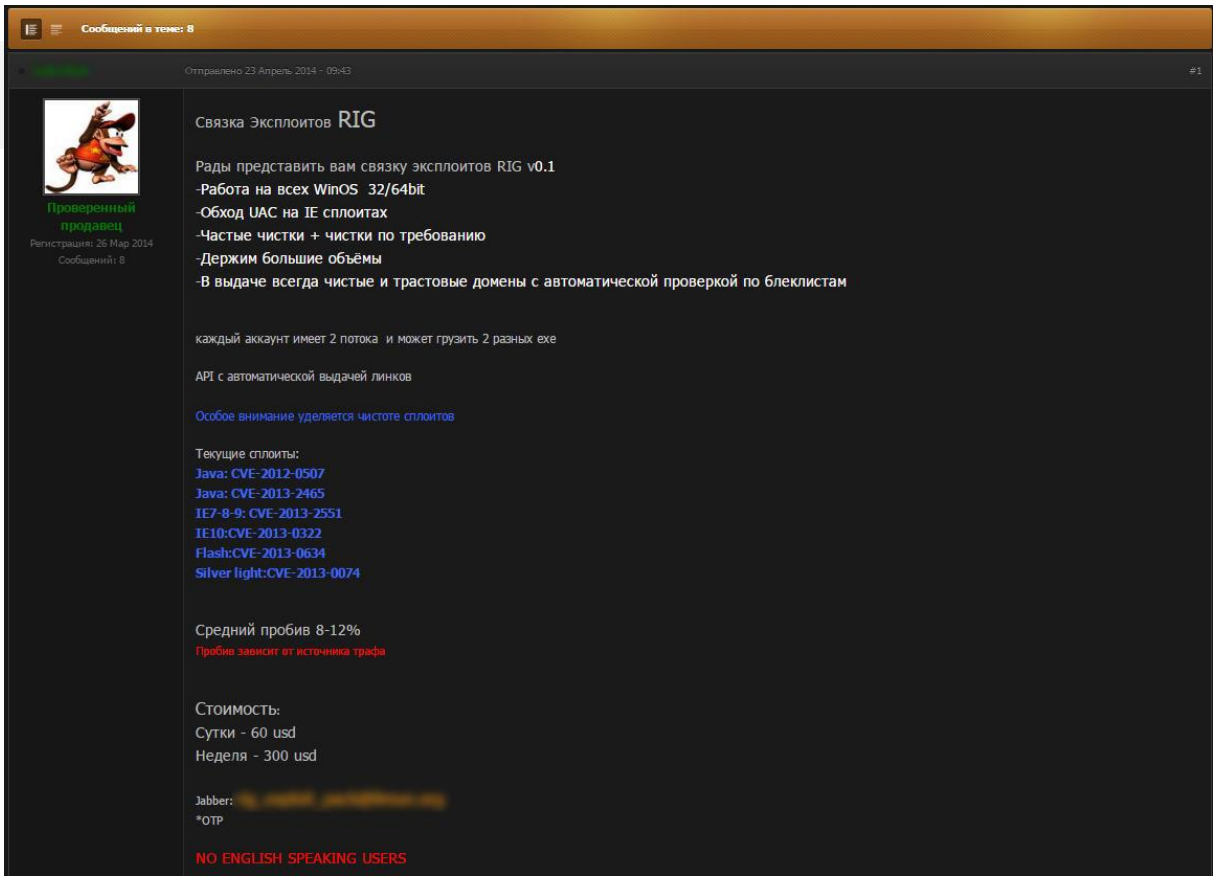


Figura 3: Publicación de foro que publicita el paquete de explotación RIG en Rusia

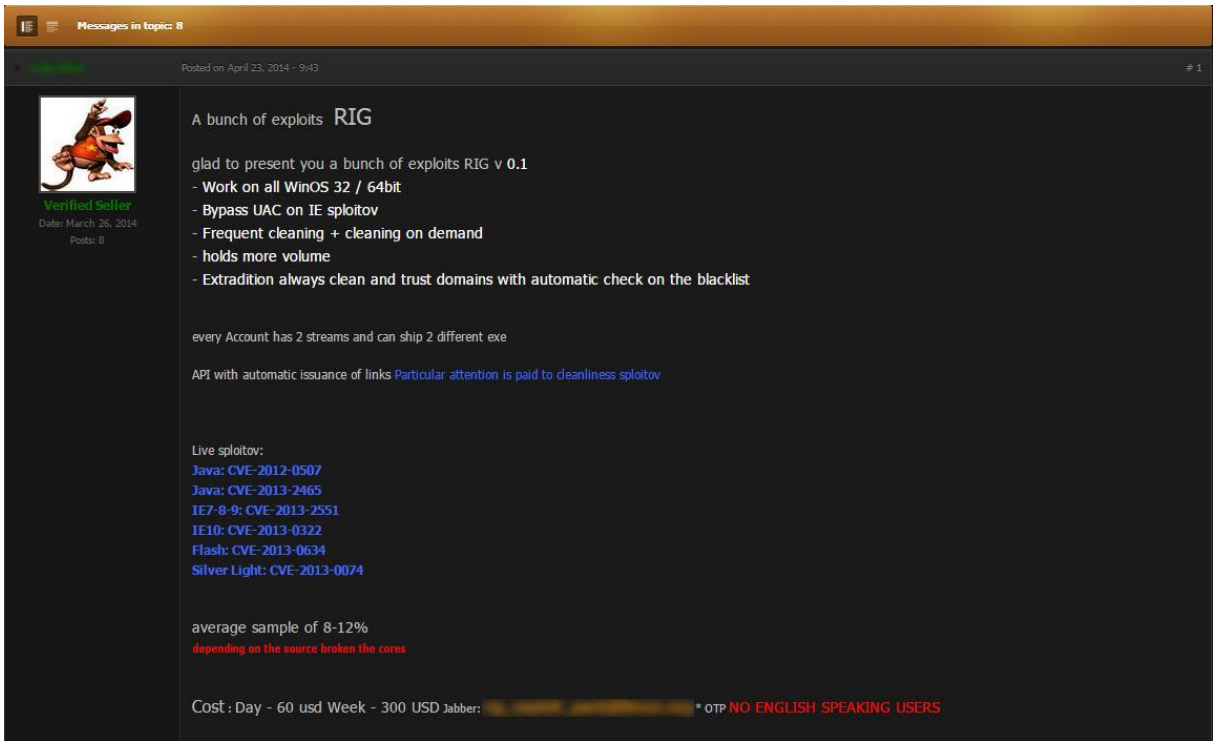


Figura 4: Traducción de la publicación de foto anterior

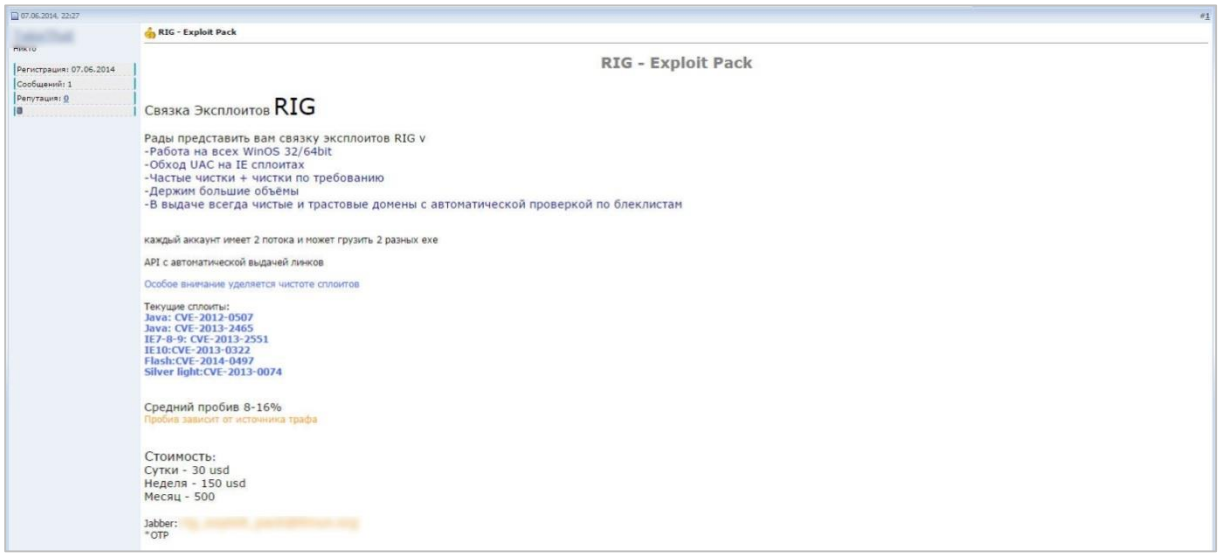


Figura 5: Publicación de foro adicional que publicita el paquete de explotación RIG

Tras realizar una evaluación más exhaustiva, se cree que solo existe una versión del kit de explotación RIG. No se ha encontrado ningún análisis del código aún, pero existe un informe sobre la filtración del código fuente en el sitio web MalwareTech que resume la cuestión de la siguiente manera:

"*Debido a la forma en que funciona el paquete de explotación RIG, el aprovechamiento se realiza mediante un servidor de back-end, de modo que no hay explotaciones dentro de la filtración*".

Puede encontrar información adicional sobre este kit de exploración en la siguiente dirección: https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2015-0311

https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2014-6332

EN EL FRENTE DEL FRAUDE

SERVICIOS DE BÚSQUEDA Y PROVEEDORES DE PII

Los analistas de inteligencia de RSA FraudAction detectaron recientemente una serie de proveedores en el entorno clandestino que ofrecen información personal y credenciales para el Reino Unido; como fechas de nacimiento, información de pasaportes del Reino Unido, escaneos de pasaportes del Reino Unido, conjuntos completos de información personal del Reino Unido, además de "fullz": datos completos de tarjetas de crédito robados junto con información de identificación personal (PII). Estos recursos ayudan al estafador a realizar transacciones fraudulentas que implican ingeniería social para sortear medidas de autenticación y autorización, y lograr su objetivo de sacar dinero de los datos de tarjetas de crédito robados y de las cuentas en línea expuestas.

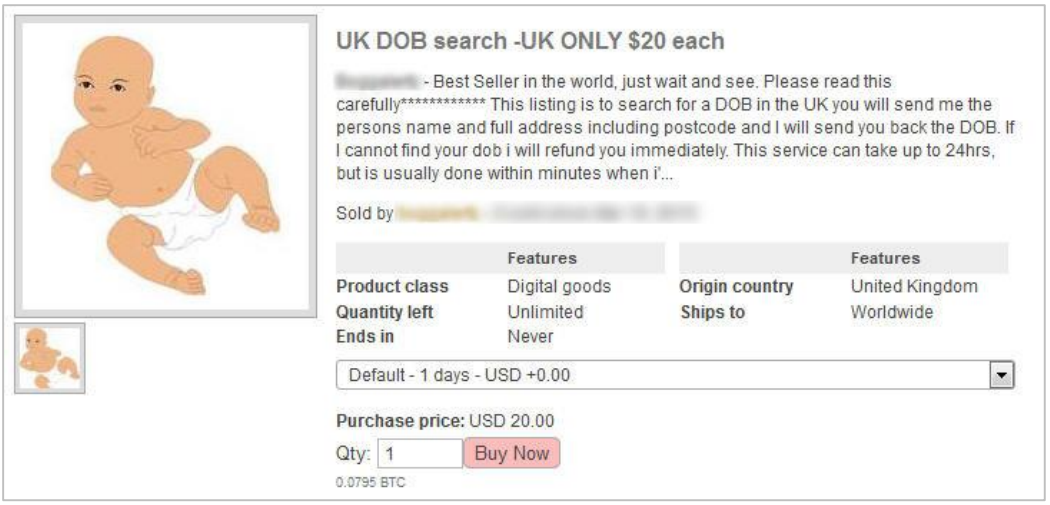


Figura 6: Información sobre fechas de nacimiento del Reino Unido a la venta

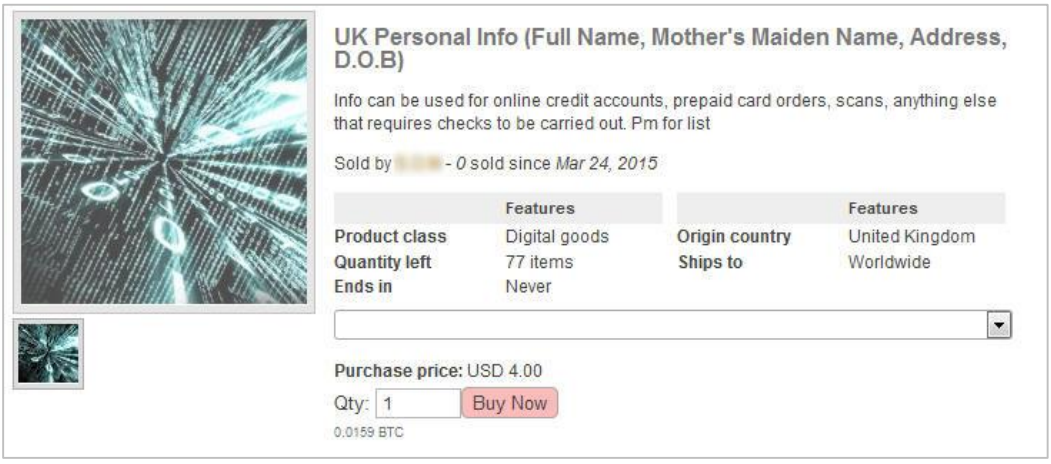


Figure 7: Información personal del Reino Unido a la venta

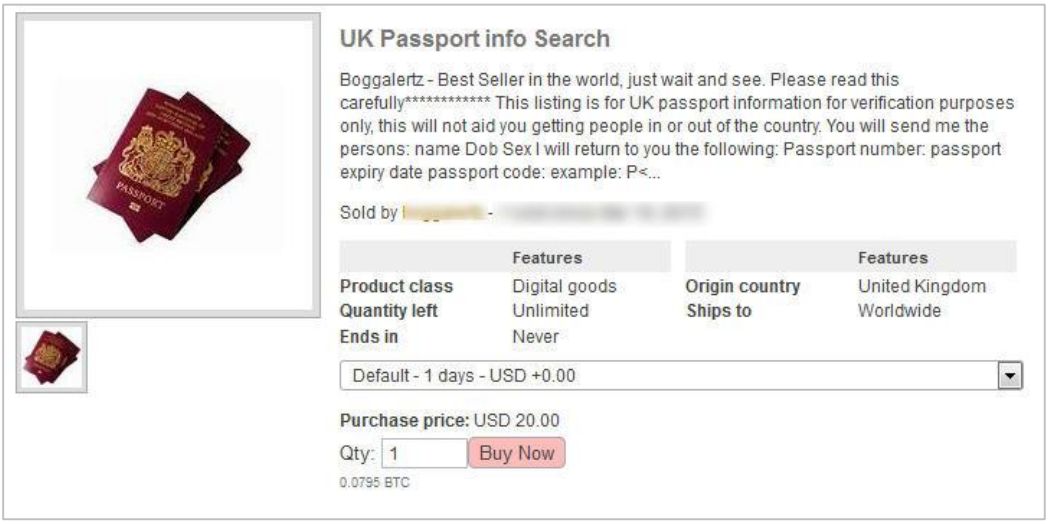


Figure 8: Venta de credenciales de pasaportes del Reino

Figure 9: Venta de escaneos de pasaportes del Reino Unido

Figure 10: Venta de "fullz" de "buena calidad" del Reino Unido

GUÍAS DE USUARIO SOBRE FRAUDE DE APUESTAS Y JUEGOS EN LÍNEA

Los analistas de inteligencia de FraudAction descubrieron un par de guías en el entorno clandestino sobre cómo estafar sitios de apuestas en línea. Una guía se publicita como un folleto de 48 páginas con un costo de US$200. La otra es un conjunto informar de consejos y trucos. Aunque estas guías ya tengan al menos 2 años, algunos de los consejos del ejecutor de la amenaza aún pueden ser pertinentes para los defraudadores, por ejemplo:

- Las mejores son las salas de juego (en línea) europeas, ya que aceptan prácticamente cualquier información personal substituta del titular de la tarjeta de crédito (por ejemplo, nombre y dirección).
- Mejores países para realizar fraude de casinos en línea: España (ES), Francia (FR), Alemania (DE), Austria (AU), Italia (IT) y (FI) Finlandia.
- Países problemáticos: EE. UU., Reino Unido, Canadá.
- El ejecutor de la amenaza enumera algunos sitios de póker en línea que aceptan tarjetas de crédito de Estados Unidos: SportsBook Poker, PlayersOnly Poker, Carbon Poker, Poker Stars, Bodog Poker, Only Poker, Super Book Poker, Full Tilt.
- Siempre revise que la tarjeta que utilice siga siendo válida y que tenga suficiente saldo disponible.
- Se recomiendan las salas de apuestas en línea con un límite superior a US$600, ya que es más probable que pierda en salas con un límite inferior.

El ejecutor de la amenaza también proporciona consejos detallados sobre cómo administrar cuentas en las salas de póker en línea, cómo depositar y retirar fondos y cómo transferir fondos entre cuentas.

En su último comentario, el ejecutor de la amenaza le recuerda a sus pares que la mayoría de los sitios de juegos tienen una vulnerabilidad o punto débil de algún tipo, y que encontrarlo y aprovecharlo depende de ellos.

LOS DEFRAUDADORES AGREGAN WHATSAPP A SUS OPCIONES DE COMUNICACIÓN

Los analistas de inteligencia de FraudAction advirtieron recientemente un defraudador que publicitaba datos de tarjetas de crédito robados, cuentas expuestas y herramientas para realizar fraudes cibernéticos. Además de los métodos estándares de comunicación mediante servicios de mensajería en línea, correo electrónico y Skype, el ejecutor de esta amenaza agregó un número de teléfono para que lo contactaran mediante la aplicación para teléfonos inteligentes Whatsapp.

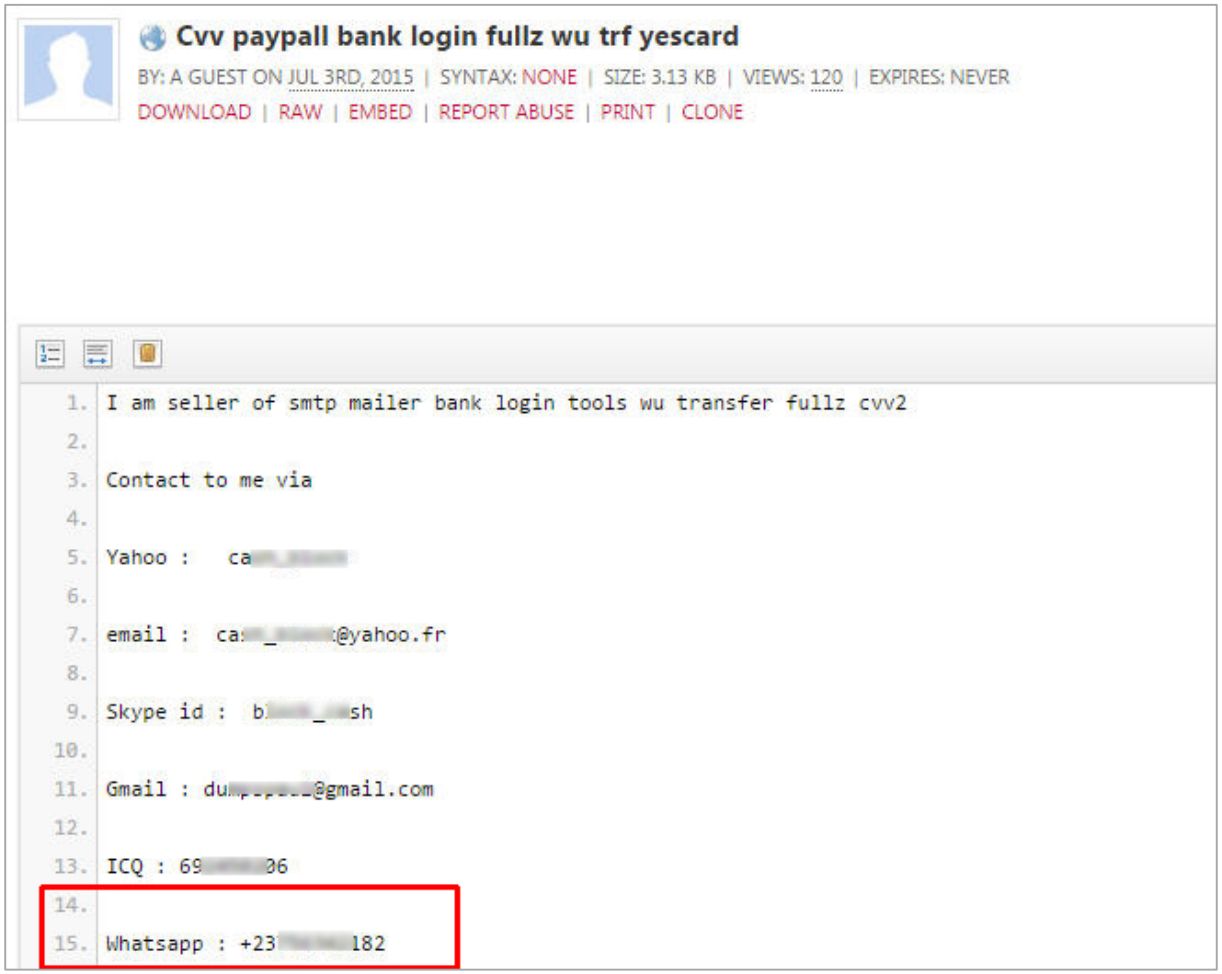


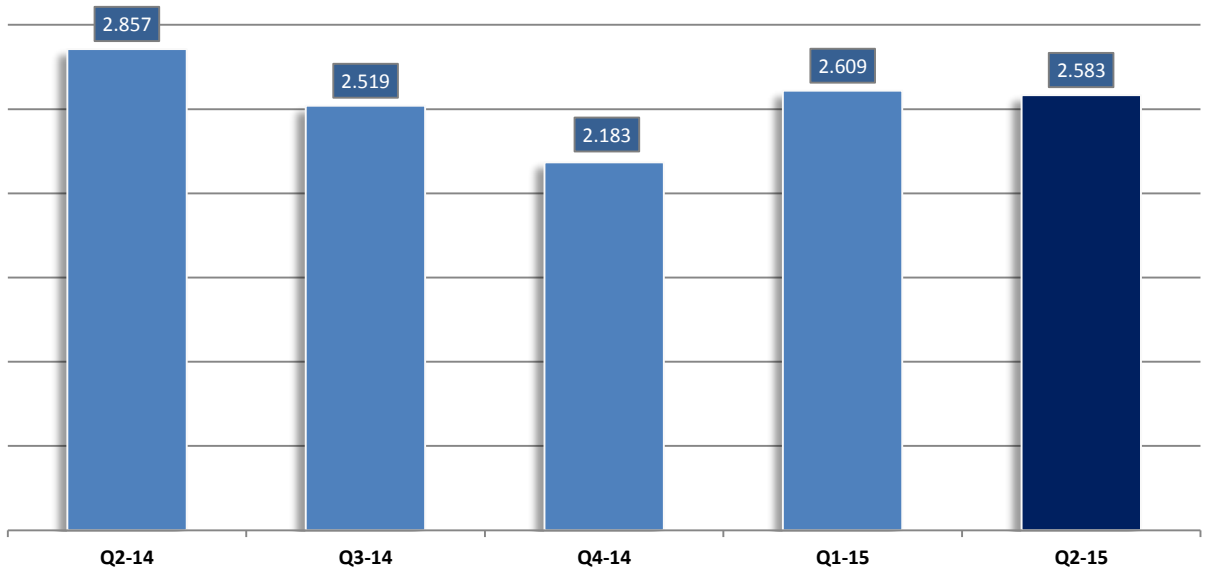
Figura 11: Número de Whatsapp ofrecido como opción de contacto

ESTADÍSTICAS DE MALWARE

Los siguientes gráficos indican la actividad global de elementos de malware troyanos registrados por RSA en los últimos cinco trimestres.

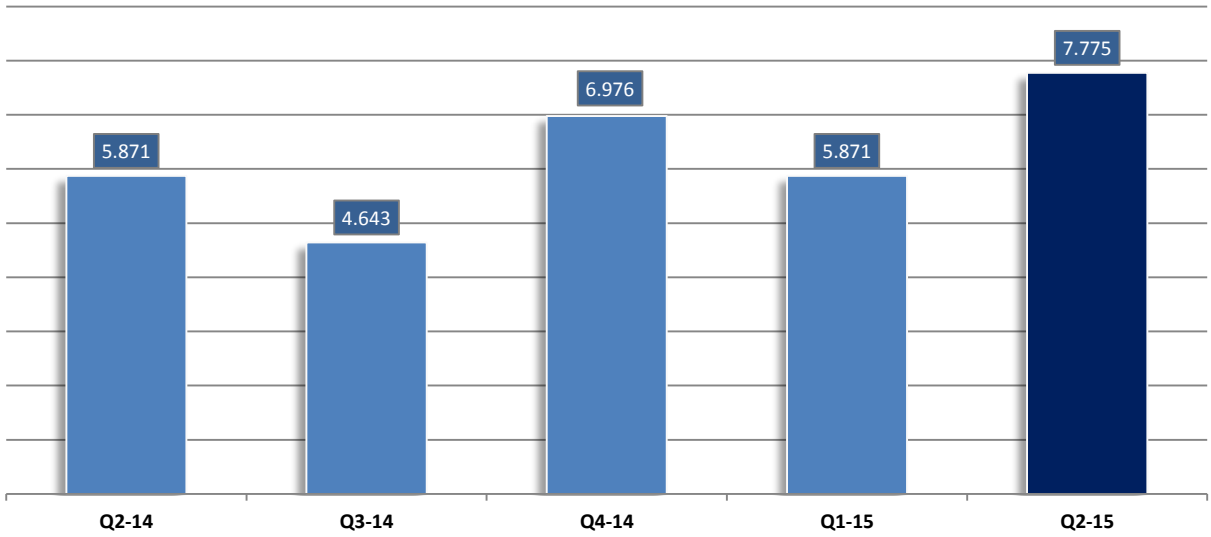
VARIANTES POR TRIMESTRE

El siguiente gráfico muestra el conteo de variantes únicas de troyanos bancarios detectadas por RSA.



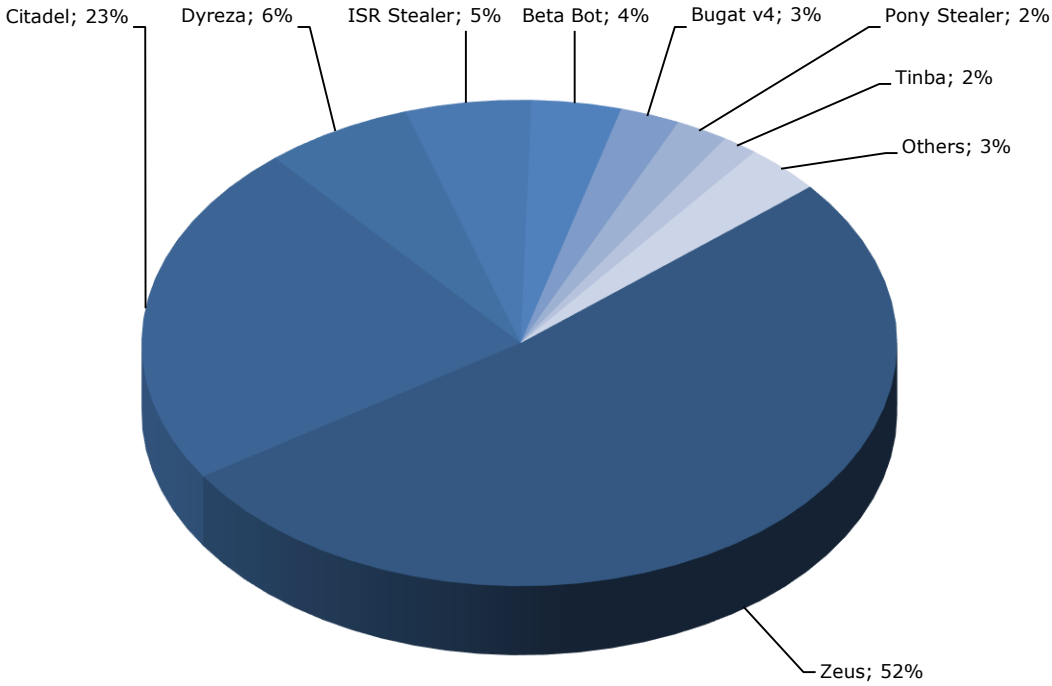
PUNTOS DE COMUNICACIÓN ÚNICOS DE TROYANOS: URL POR TRIMESTRE

Un conteo de puntos de comunicación (URL) utilizados para *infección*, *actualización* o como *puntos de lanzamiento* en ataques de troyanos en todo el mundo. Cada ataque de troyano puede utilizar varios puntos de comunicación, por lo tanto, la cantidad de puntos de comunicación relacionados con troyanos únicos siempre será *considerablemente mayor* que la cantidad de variantes únicas detectadas.



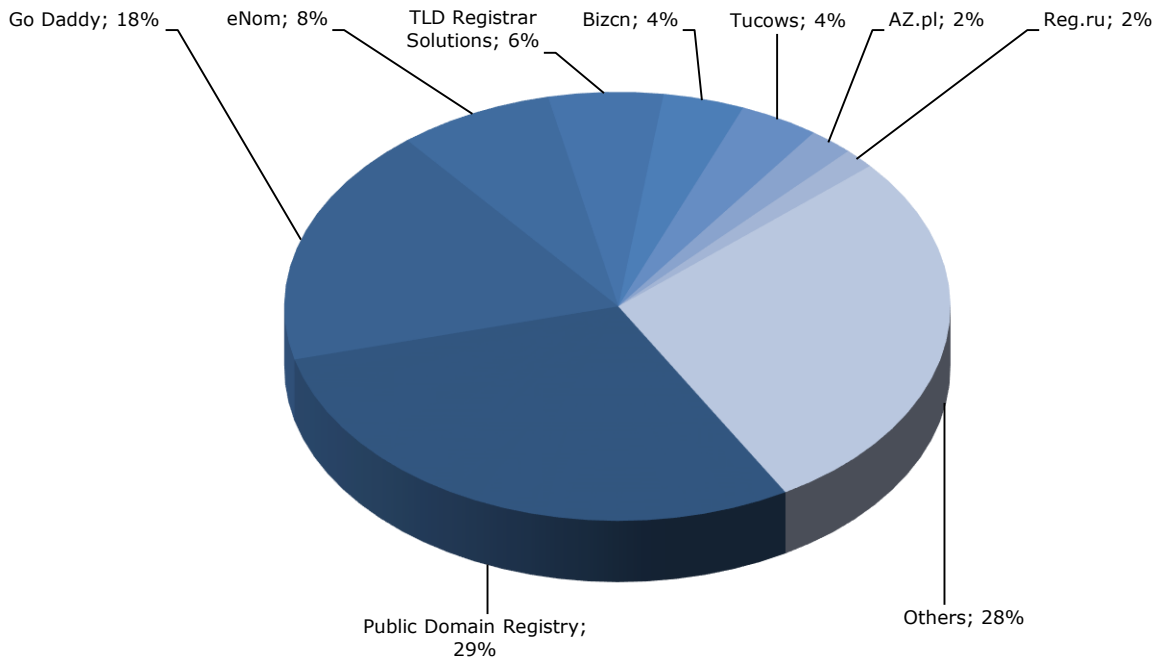
DISTRIBUCIÓN GLOBAL DE FAMILIAS DE TROYANOS

La siguiente tabla muestra la distribución de varias familias de troyanos responsables de ataques a entidades en todo el mundo en el segundo trimestre de 2015, como lo detectó el centro de control antifraude de RSA (AFCC). Zeus sigue monopolizando el escenario global, pero su protagonismo se redujo en relación con el trimestre anterior (-15 %), mientras que Citadel (+1 %), Dyreza (+2 %) y Bugat v4 (+1 %) siguieron creciendo. Tinba (Tiny Banker, detectado por primera vez en mayo de 2012) reapareció en los últimos 6 a 8 meses y alcanzó un 2 % de la participación de la distribución global de troyanos.



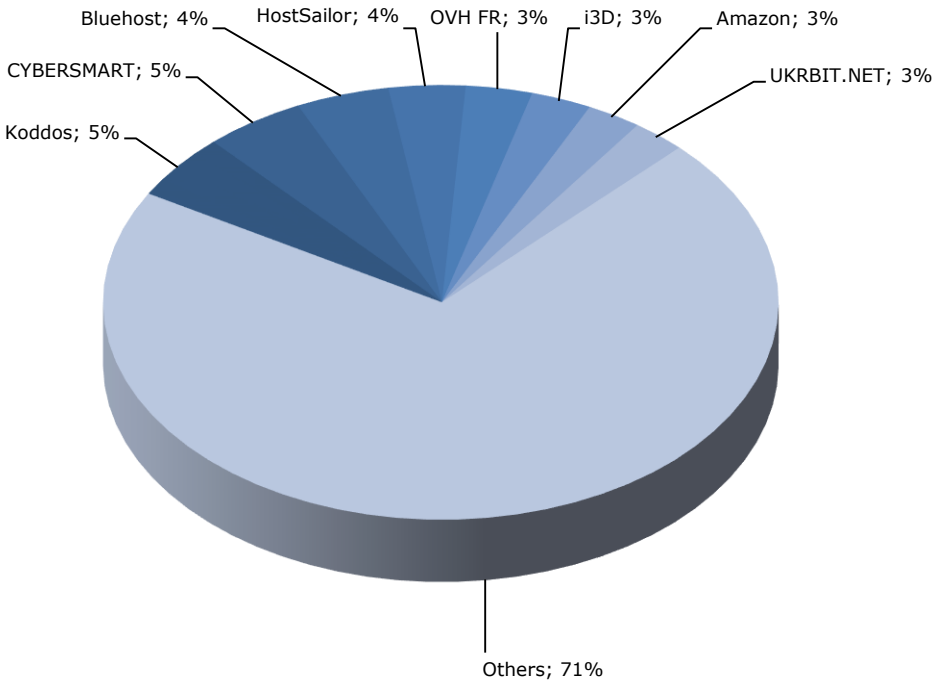
PRINCIPALES REGISTRADORES DE DOMINIOS DE TROYANOS

El siguiente gráfico muestra una vista proporcional de los registradores con los cuales se registraron las mayores cantidades de dominios de comunicación de troyanos durante el segundo trimestre de 2015. Los botmasters troyanos suelen comprar uno o más dominios para alojar sus recursos de comunicación.



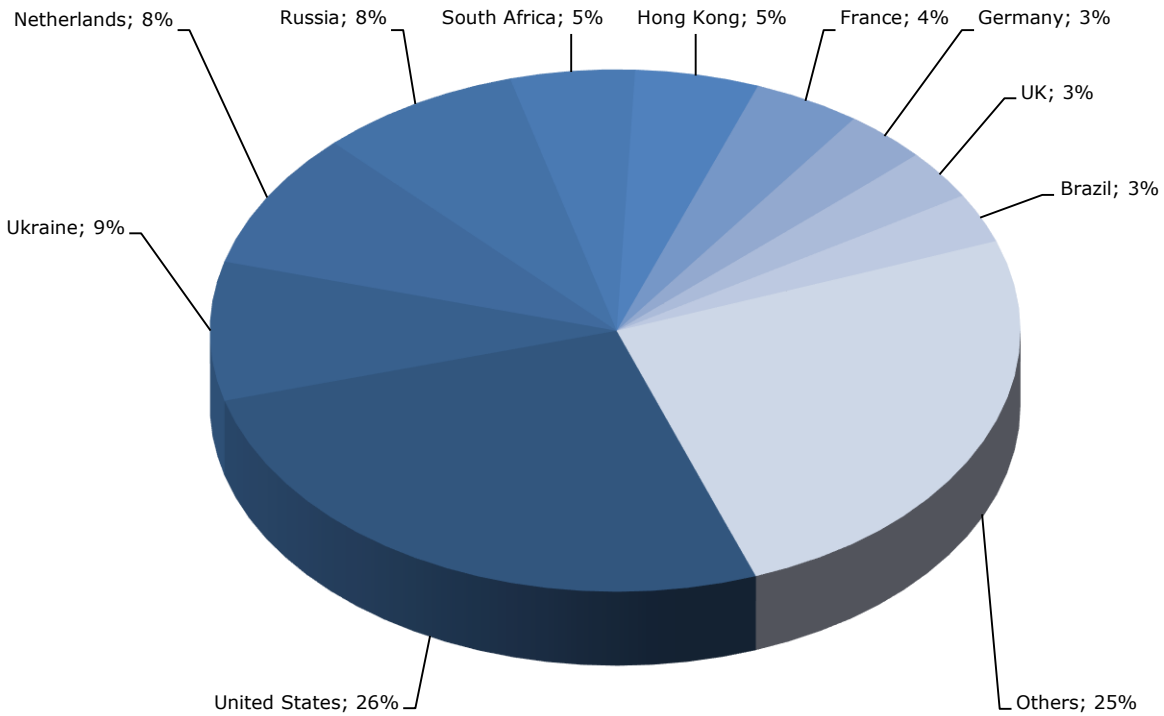
PRINCIPALES ISP QUE ALOJAN TROYANOS

El siguiente gráfico muestra una vista proporcionar de los ISP que han alojado la mayor cantidad de recursos de comunicación de troyanos en el segundo trimestre de 2015. Tenga en cuenta que los relativamente nuevos servicios de alojamiento web de Amazon ya se están utilizando para alojar malware.



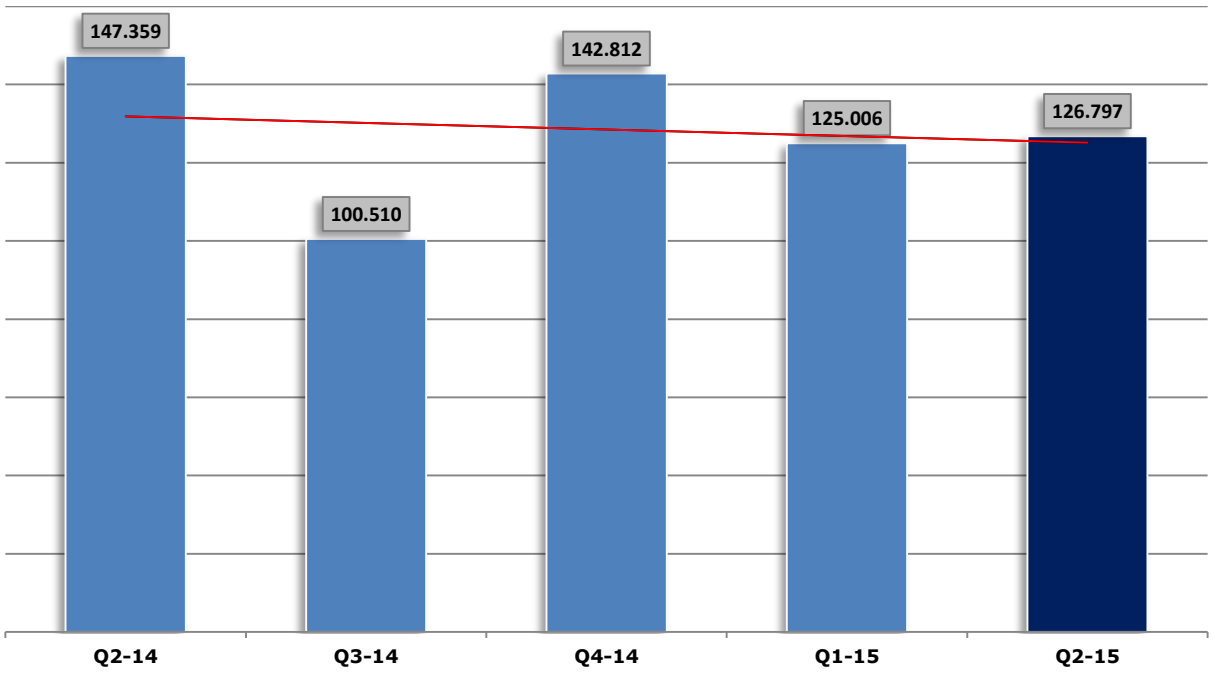
PRINCIPALES PAÍSES QUE ALOJAN TROYANOS

Principales países según la porción de URL de comunicación de troyanos que alojaron durante el segundo trimestre de 2015. Los países de servicio de alojamiento se determinan por la ubicación del ISP o la ubicación física del registrador de dominios.



ESTADÍSTICAS DE ROBO DE IDENTIDAD

En el segundo trimestre de 2015, RSA registró un total de **126,797** ataques de robo de identidad en el mercado global. Este volumen representa un incremento del **1 %** respecto del trimestre anterior y una caída del **14 %** respecto del segundo trimestre de 2014.

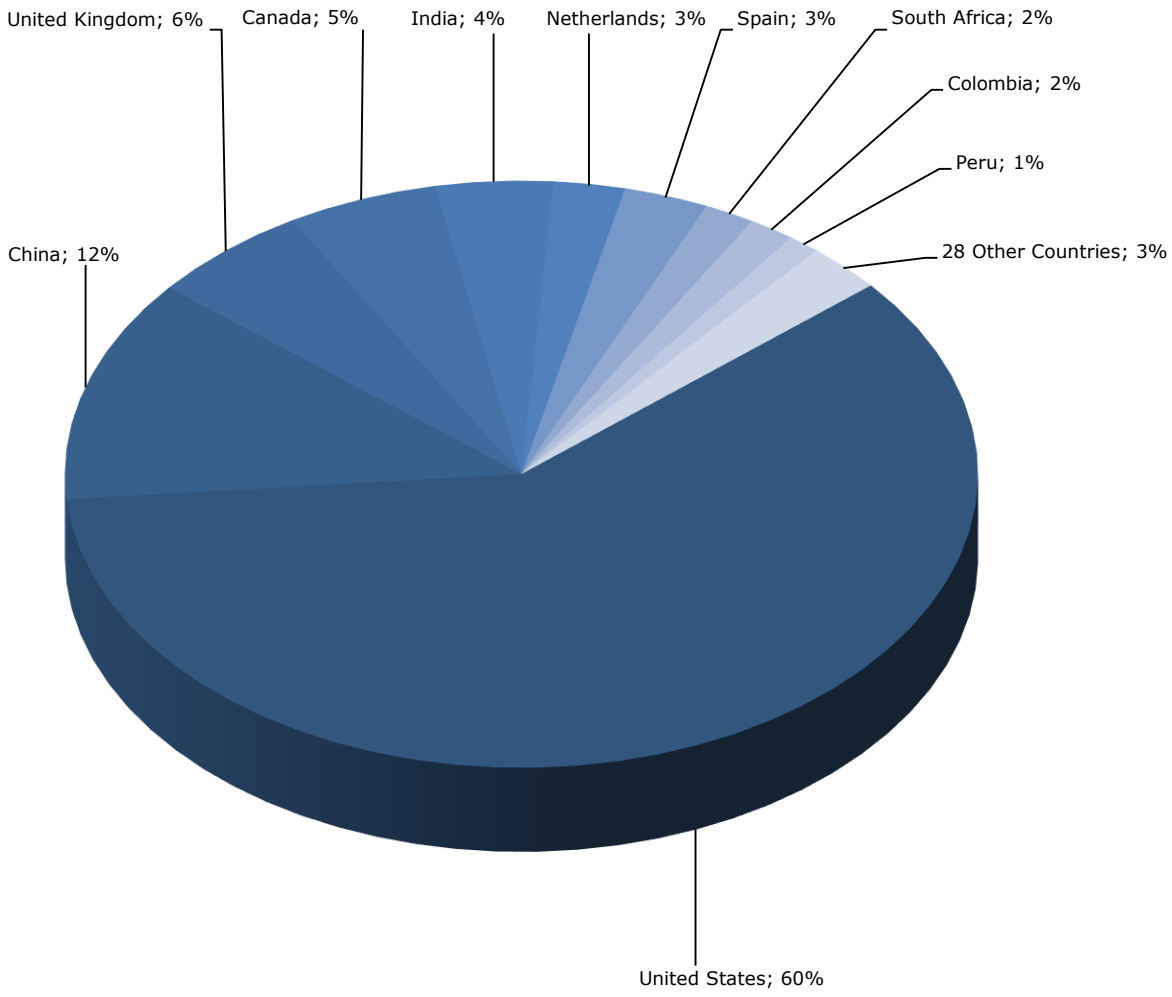


VOLÚMENES DE ATAQUE DE ROBO DE IDENTIDAD GLOBALES

En el segundo trimestre de 2015, Estados Unidos conservó su lugar como el país más atacado en el gráfico, con un 60 % de los ataques de robo de identidad globales.

China pasó al segundo lugar con un 12 %, el Reino Unido se ubicó en el tercer puesto con un 6 %, Canadá descendió al cuarto puesto con un 5 %, India se ubicó en el quinto lugar con un 4 % de participación, los Países Bajos y España ocuparon el sexto lugar con un 3 % cada uno, Sudáfrica y Colombia se ubicaron en el séptimo puesto con un 2 % cada uno y Perú quedó en el octavo lugar con el 1 % del total de los volúmenes de ataque de robo de identidad a nivel mundial.

Veintiocho países adicionales absorbieron el 3 % restante, cada uno con menos del 1 % de los ataques.

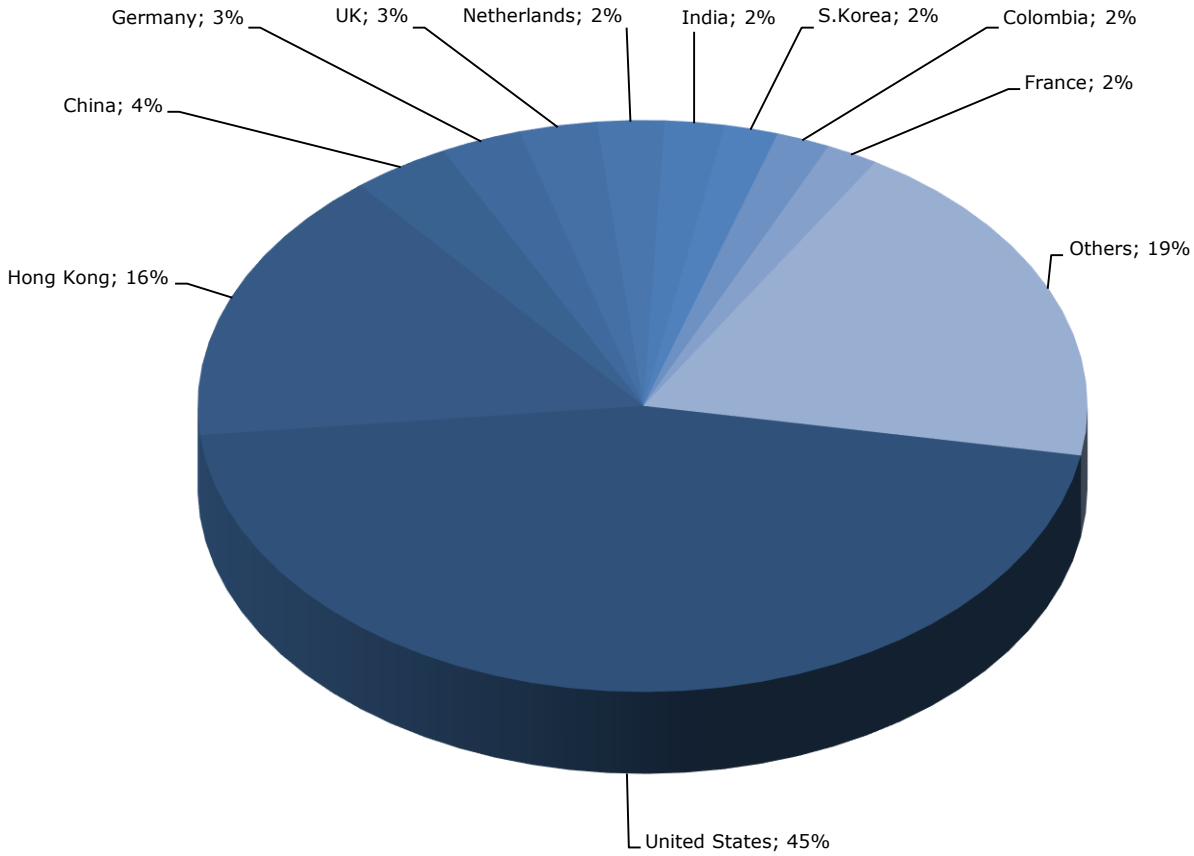


PAÍSES PRINCIPALES QUE ALOJAN ROBO DE IDENTIDAD

En el segundo trimestre de 2015, Estados Unidos conservó el primer lugar, con un 45 % de los ataques de robo de identidad globales.

Hong Kong se ubicó en el segundo lugar, China en el tercero , Alemania y el Reino Unido compartieron el cuarto lugar, y los Países Bajos, India, Colombia y Francia compartieron el quinto lugar.

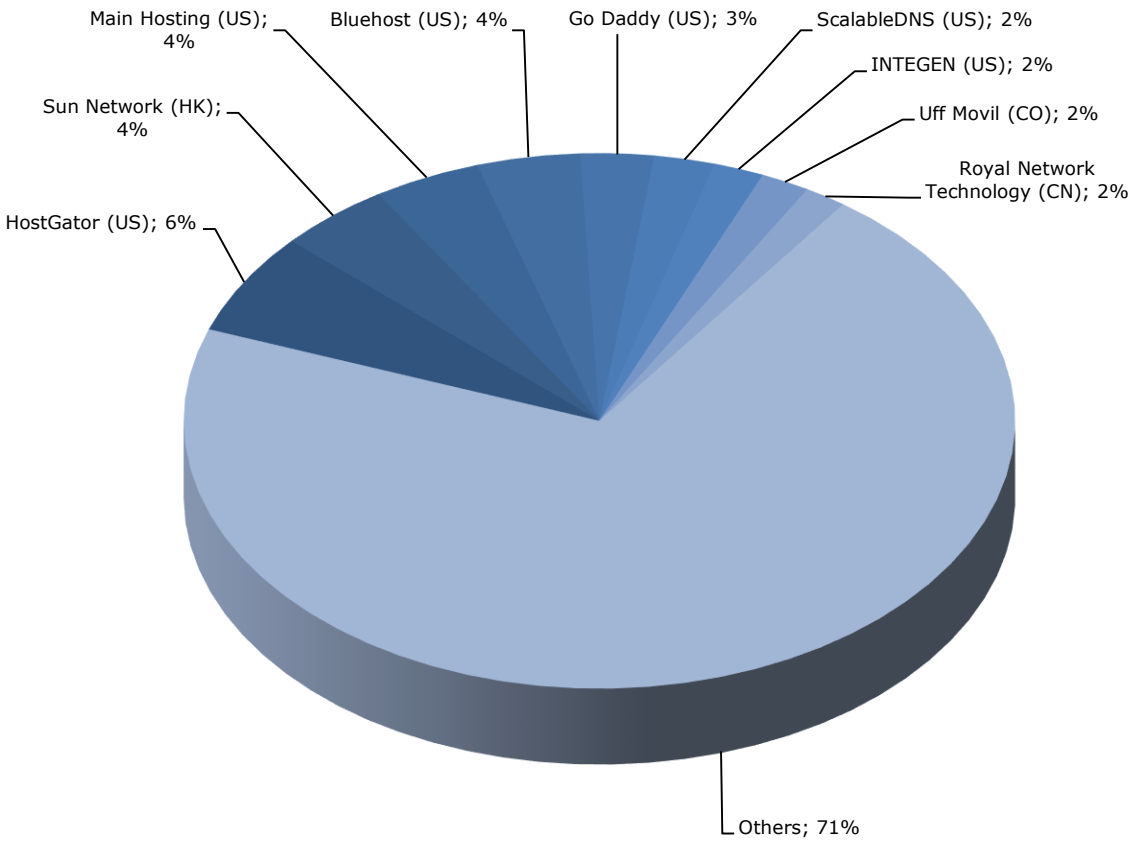
Los ISP de 70 países adicionales alojaron el 19 % restante de los ataques de robo de identidad del mundo.



PRINCIPALES ISP QUE ALOJAN ROBO DE IDENTIDAD

En el segundo trimestre de 2015, HostGator ocupó el primer lugar entre los ISP de alojamiento, Sun Network, Main Hosting y Bluehost compartieron el segundo lugar, GoDaddy se ubicó en la tercera ubicación y Scaleable DNS, Integen, Uff Movil y Royal Network Technology compartieron el cuarto lugar.

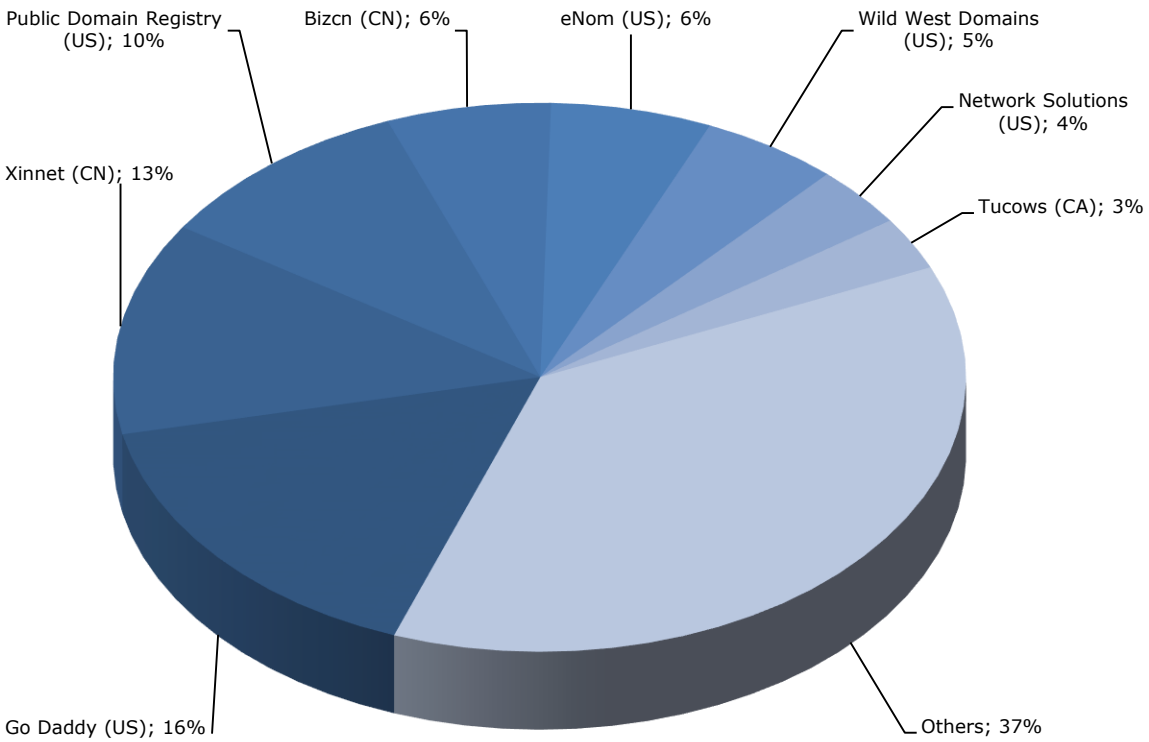
Los 1,191 ISP restantes alojaron el 71 % restante del volumen global de los ataques de robo de identidad, ya que cada uno alojó un 1 % o menos de los ataques.



REGISTRADORES PRINCIPALES QUE ALOJAN ROBO DE IDENTIDAD

En el segundo trimestre de 2015, GoDaddy lidera el gráfico con un 16 % de participación, Xinnet está en segundo lugar, Public Domain Registry está en tercer lugar, Bizcn y eNom comparten el cuarto lugar, Wild West Domains están en la quinta posición, Network Solutions se ubica en el sexto lugar y Tucows en la séptima ubicación.

Otros 232 registradores adicionales contribuyeron con el 37 % restante de los registros de dominios de ataques.



POR SI PASÓ ALGO POR ALTO

A continuación, figura un resumen de todos los informes que enviamos a nuestros clientes en los últimos meses.

INFORMES DE AMENAZAS DE FRAUDACTION

Los siguientes **Informes de amenazas** incluyen nuestros hallazgos más recientes del cibercrimen clandestino y se enviaron a nuestros clientes entre enero y junio de 2015:

Nombre de archivo del informe	Resumen
TR150115 Falsificación de códigos de autorización bancarios para transacciones rechazadas	Un estafador descubre un método para generar códigos de autorización que se asemejan a códigos de autorización bancarios reales, y utiliza tarjetas de crédito canceladas en un esquema de 'pago forzoso' para estafar comerciantes.
TR150125 Estafador hace alarde sobre trucos de 3D Secure	Un estafador afirma haber descubierto un método para sortear un paso de autorización en el procesamiento de transacciones de 3D Secure.
TR150201 Project Sniffer: un nuevo malware POS a la venta	**Project Sniffer**, una nueva aplicación de malware POS se publicita en el entorno clandestino.
TR150208 Criminal del robo de identidad con capacidad de respuesta: oferta de kits de robo de identidad para varias plataformas	Un estafador publicita la venta de un kit de robo de identidad que admite varias plataformas y proporciona servicio y soporte completos.
TR150210 El uso de spam para ocultar la apropiación de cuentas	Campaña de spam utilizada para ocultar la notificación de cambio de correo electrónico en una apropiación de cuenta.
TR150211 Estafador ofrece tiendas todo en uno de comercio electrónico	Un estafador ofrece tiendas en línea completamente personalizadas falsas con conexiones a gateways de pago para fines de fraude de comercio electrónico.
TR150215 Curso sobre estafadores: Cómo exponer la administración de CC en línea	Un estafador comparte con sus pares un curso sobre cómo obtener acceso al servicio de administración en línea de la tarjeta de crédito de un banco importante, lo que incluye un método para un cambio de dirección de facturación fraudulento.
TR150215 Fraude comparte publicidad de la plataforma Voxis	Un miembro de un foro clandestino demuestra interés en la plataforma **Voxis**: un método automatizado de extracción de efectivo para fraudes. El estafador también brinda un vínculo al sitio en el cual se vende la plataforma.
TR150217 Consejos de un estafador para actualizar CVV a FULLZ	Consejos de un estafador sobre cómo mejorar datos de tarjetas de crédito robados mediante ingeniería social y búsquedas de código abierto para obtener credenciales adicionales de las víctimas

Nombre de archivo del informe	Resumen
TR150222 Fraudfox VM: Una nueva herramienta para falsificar huellas digitales de navegador	**FraudFoxVM** se publicita en el entorno clandestino como una nueva herramienta para falsificar elementos de huella digital de navegador en un intento de sortear medidas de seguridad de autenticación.
TR150223 Estafador comparte una nueva herramienta para robar contraseñas: _zStealer	**Z*stealer**: Una nueva herramienta para robar contraseñas e información de inicio de sesión de varias aplicaciones en línea está a la venta en el entorno clandestino.
TR150223 Consejos de un estafador: Cómo establecer ubicaciones físicas de lanzamiento	Un estafador proporciona una guía detallada para configurar direcciones/ubicaciones de lanzamiento de operaciones fraudulentas en el Reino Unido.
TR150310 WIN Código fuente del ransomware WIN Locker a la venta	Un estafador ofrece la venta de código del **ransomware WIN Locker** y un demo en vivo del ransomware.
TR150319 Nueva información sobre criminales del robo de identidad con capacidad de respuesta	Actualización del informe "Criminal del robo de identidad con capacidad de respuesta": 3 alias vinculados a un ejecutor de amenaza, historial de 4 años de actividad fraudulenta, kits de robo de identidad dirigidos a bancos del Reino Unido.
TR150331 Nuevo malware DarkPOS a la venta en el entorno clandestino	**DarkPOS**, una nueva aplicación de malware que apunta a POS, se publicita en el entorno clandestino.
TR150331 Estafadores debaten sobre cómo atacar un procesador de pagos	Estafadores analizan un esquema para atacar el servicio de procesamiento de pagos Authorize.net, que incluye un método de extracción de dinero de datos de tarjetas de crédito robados mediante la transferencia a cuentas bancarias de los estafadores.
TR150426 Estafador recomienda atacar LiqPay para obtener dinero de tarjetas de crédito	Un estafador recomienda utilizar un portal de operaciones bancarias en línea legítimo en Ucrania para transferir y extraer dinero con los datos robados de tarjetas de crédito.
TR150427 Cómo utilizar gofundme para obtener dinero de tarjetas de crédito	Un estafador ofrece un método para utilizar un sitio de financiación colectiva para retirar fondos de los datos de tarjetas de crédito robados
TR150430 Publicidad de la botnet DiamondFox también conocido como Gorynych	La botnet Gorynych cambió de nombre y está a la venta en el entorno clandestino como DiamondFox.
TR150505 Estafador vende tarjetas prepagadas de Italia	Un estafador ofrece la venta de tarjetas prepagadas italianas en el entorno clandestino. Las tarjetas se pueden utilizar como una cuenta de lanzamiento de lavado de dinero, para la transferencia de fondos y como medio de extracción de dinero.
TR150506 Estafador vende scripts de tiendas	Un estafador ofrece scripts para tiendas en línea automatizadas a otros estafadores
TR150521 DD4BC: Extorsión mediante DDoS	El grupo DD4BC intenta obtener de forma extorsiva pagos de Bitcoin de empresas mediante amenazas sobre ataques DDoS

Nombre de archivo del informe	Resumen
TR150630 Nueva plataforma de compra en el mercado clandestino	Un mercado clandestino establecido crea una plataforma automatizada para vender datos de tarjetas y cuentas expuestas.

INFORMES SOBRE TROYANOS

Los siguientes **informes de troyanos** incluyen nuestros hallazgos más recientes sobre el malware detectado en libre circulación y se enviaron a nuestros clientes entre enero y junio de 2015:

Nombre de archivo del informe	Resumen
ATS_150215 Hesperbot para dispositivos móviles (Android)	La parte 2 incluye una serie de artículos sobre el troyano **Hesperbot**, en este informe que es un análisis de la versión móvil del malware.
ATS_150216 Nuevos ataques a Boleto mediante BolFox	Un nuevo vector de amenaza que ataca a los usuarios de **Boleto** en Brasil mediante una extensión del navegador Firefox denominada **BolFox** que roba información y reemplaza información de formularios de Boleto.
ATS_150217 Esquema de redes sociales utilizado para propagar malware	**Intermediarios en redes sociales** Variante de malware utiliza Facebook para distribuir malware
ATS_150325 Análisis dinámico del malware PoSeidon	Análisis dinámico de una nueva variante de malware llamada **PoSeidon** que ataca sistemas POS.
ATS_150518 Un análisis dinámico de Gorynych (también llamado DiamonFox)	Un análisis dinámico del malware **Gorynych**, que recientemente cambió su nombre y ahora se llama **DiamondFox**.
ATS_150629 Nueva ola de troyanos en documentos Word	Los analistas de RSA descubrieron documentos Word en correos electrónicos que tienen el troyano **Zeus** incorporado directamente en el documento.

ACERCA DE RSA

RSA, la División de Seguridad de EMC, es el principal proveedor de soluciones de seguridad, riesgo y administración de cumplimiento de normas para la aceleración del negocio. RSA ayuda a las principales organizaciones del mundo a alcanzar el éxito solucionando sus retos de seguridad más complejos y confidenciales. Entre estos retos, se incluyen la administración de los riesgos organizacionales, la protección de la colaboración y del acceso por medio de dispositivos móviles, la comprobación del cumplimiento de normas y la protección de ambientes virtuales y de nube.

Mediante la combinación de controles fundamentales para los negocios en verificación de identidad, cifrado y
administración de claves, SIEM, prevención de pérdida de datos y protección contra fraudes con funciones eGRC líderes del sector y servicios

EMC², EMC, RSA y el logotipo de RSA son marcas registradas o marcas comerciales de EMC Corporation en los Estados Unidos y en otros países. Todas las demás marcas comerciales utilizadas en este documento pertenecen a sus respectivos propietarios. ©2015 EMC Corporation. Todos los derechos reservados.
Publicado en México

mexico.emc.com/rsa (visite el sitio web de su país correspondiente)