

HISPASEC SISTEMAS
Seguridad y Tecnologías de la Información



Servicios Antitroyanos

www.hispasec.com

SERVICIO DE DETECCIÓN Y ANÁLISIS DE TROYANOS BANCARIOS

Los ataques de phishing contra entidades bancarias están evolucionando hacia técnicas cada vez más refinadas y efectivas, destacando entre ellas la cada vez mayor proliferación de troyanos bancarios. Este "malware" es creado y destinado específicamente para la captura de credenciales bancarias que permiten tener acceso a los activos de los clientes.

El coste estimado del crimen online en los Estados Unidos fue de 67.000 millones de dólares [1] en 2005, según datos del FBI. En diciembre de 2005 hasta 250.000 [2] ordenadores al día fueron infectados por algún tipo de troyano que permitía controlarlos o robar información privada.

El objetivo de este servicio es minimizar y mitigar los ataques que se basen en el uso de troyanos bancarios y que pudieran tener como objetivo a los clientes de la entidad bancaria o comercio electrónico afectado. Estos troyanos se instalan de forma inadvertida en sus sistemas y tienen acceso ilícito a sus credenciales.

A principios del 2007 el banco sueco Nordea reconoció unas pérdidas de 880.000 euros. 250 usuarios se habían visto afectados por un troyano bancario destinado al robo de datos que durante más de tres meses permitió a los estafadores obtener los activos sin ser detectados [3].

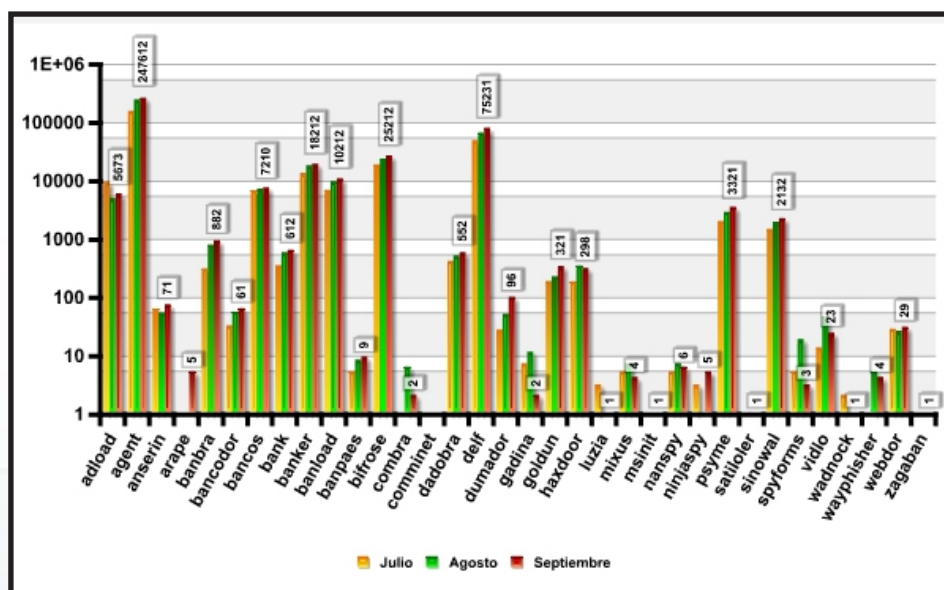
La capacidad de detección de troyanos bancarios no tiene precedentes a nivel mundial; a fines de 2008 estábamos detectando cada día 4.000 nuevas muestras en nuestro laboratorio, de las cuales seleccionamos y analizamos de forma manual unas 300, según afectan a nuestros clientes.

FAMILIAS _ □ ×

"banker", "bancos", "banger",
 "bancodor", "banbra", "banpaes",
 "bifrose", "arape", "comminet",
 "delf", "dumador", "haxdoor",
 "ninjaspy", "webdor", "combra",
 "rubank", "gadina", "getmails",
 "msinit", "psyme", "adload",
 "banload", "dadobra", "projecx",
 "vidlo", "agent", "mixus",
 "ebtreporter", "goldun", "prodoom",
 "bankfraud" y "zagaban"

familias de mayor impacto

NÚMERO DE TROYANOS POR FAMILIA (evolución de los últimos tres meses)



[1] When Online Crooks Advertise http://blog.washingtonpost.com/securityfix/2006/08/when_online_crooks_advertise.html

[2] Nearly a Quarter Million PCs Turned Into 'Zombies' Daily <http://www.technewsworld.com/story/48174.html>

[3] Entrevista con el creador de un troyano bancario <http://www.hispasec.com/unaaldia/3019>

SERVICIO DE DETECCIÓN Y ANÁLISIS DE TROYANOS BANCARIOS

De esta forma, en caso de que el Laboratorio de Investigación detecte un troyano bancario específicamente diseñado para cometer fraude contra los clientes de la entidad que tenga contratado este servicio, pondrá en marcha su protocolo de control de amenazas.

Este protocolo incluye la activación en paralelo de varios sistemas destinados a la mitigación de la amenaza desde varios frentes: estudio y análisis del troyano y aviso a la entidad.

Además, se establece una colaboración con las casas antivirus para acelerar el desarrollo de las correspondientes vacunas y actualizaciones de firmas. Esto permite una temprana detección y bloqueo por parte de los diferentes antivirus del mercado.

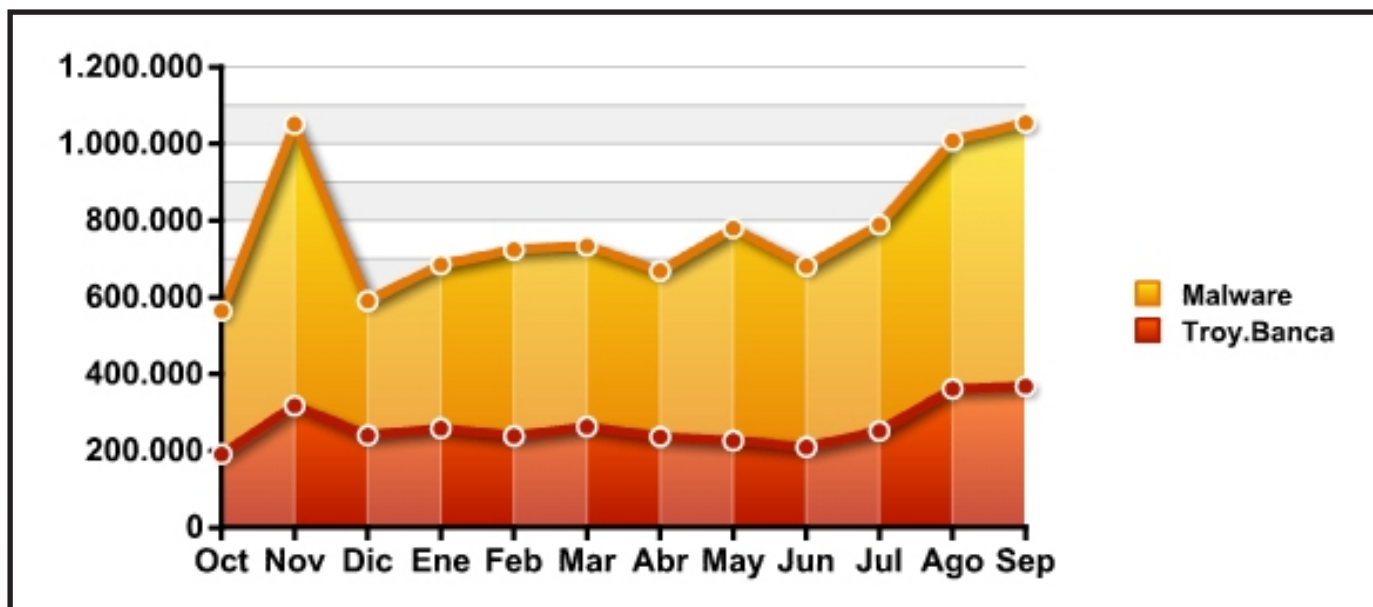
También se actuará bajo demanda cuando se detecte que algún cliente de la entidad se haya visto afectado por algún troyano, keylogger o cualquier tipo de “malware” genérico. Procediendo de igual forma al análisis del espécimen.

Entre otras, se analizan en profundidad las muestras de las familias que suponen mayor impacto en la actualidad.

RIESGOS — □ ×

- Pérdida de confianza** del cliente en los servicios de Banca Electronica.
- Pérdidas económicas** en caso de reembolso de cantidades sustraídas.
- Incremento de llamadas** al Servicio de Atención al Cliente.
- Pérdida de imagen** de la entidad.
- Gastos e inconvenientes** provocados por las denuncias.

EVOLUCIÓN DEL MALWARE DE BANCA (evolución 2007 - 2008)

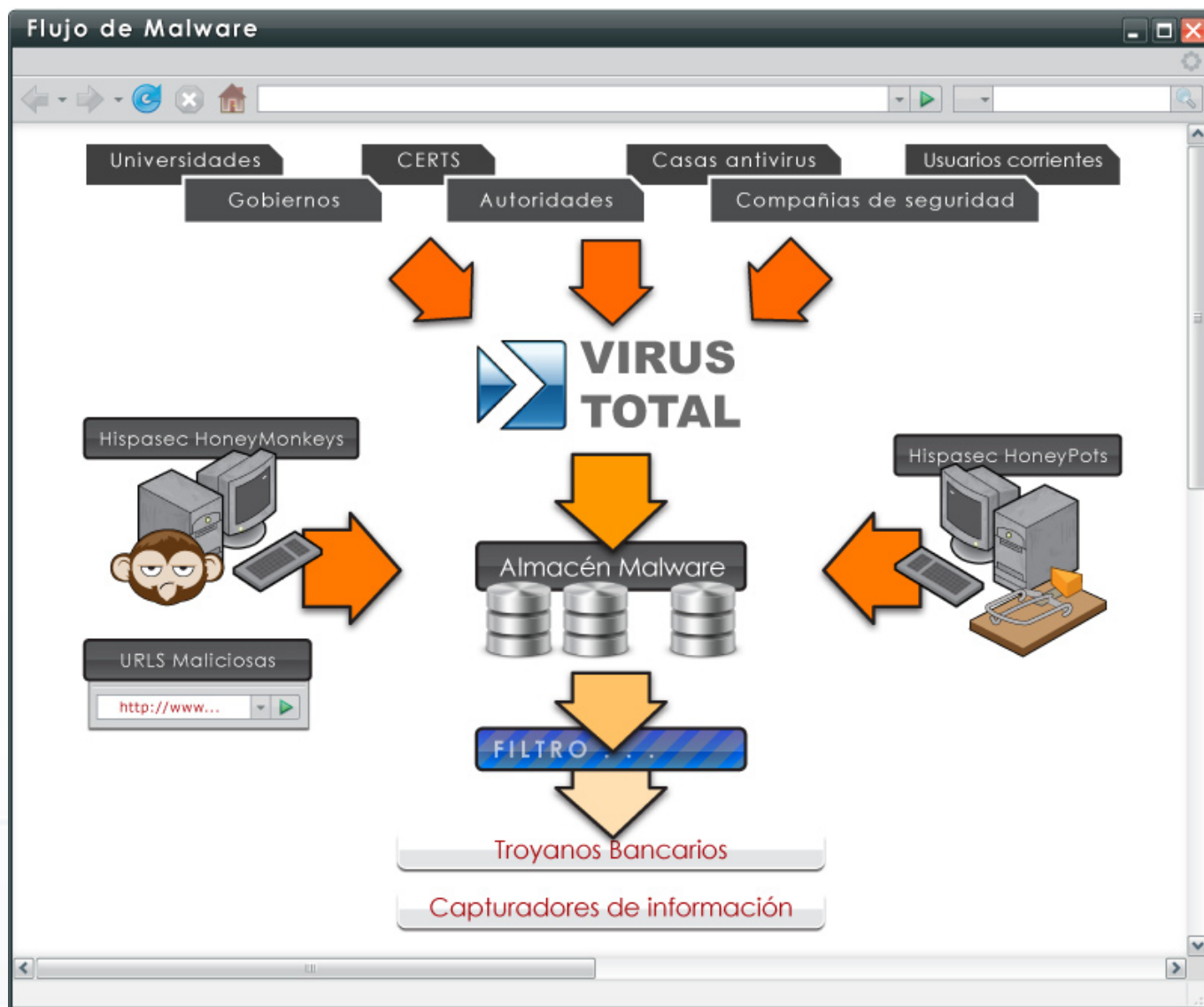


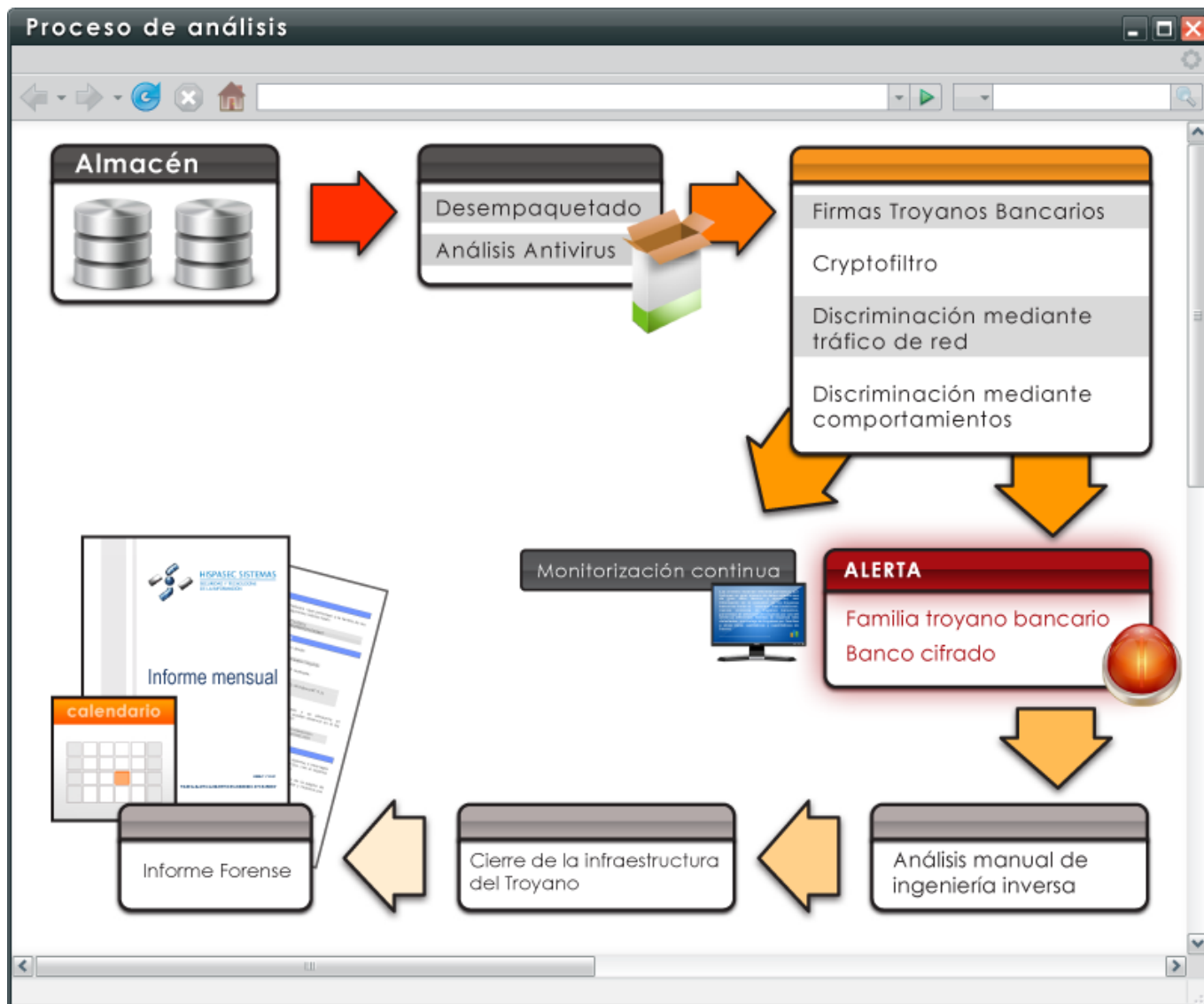
SERVICIO DE DETECCIÓN Y ANÁLISIS DE TROYANOS BANCARIOS

El servicio no sólo incluye el tratamiento y acciones ante el “malware” diseñado específicamente para afectar a los clientes de su entidad. Además, los clientes de este servicio reciben información constante sobre la evolución de este tipo de “malware”, con datos de valor sobre todos los especímenes analizadas.

Este protocolo incluye la activación en paralelo de varios sistemas destinados a la mitigación de la amenaza desde varios frentes: estudio y análisis del troyano y aviso a la entidad.

Los clientes recibirán informes periódicos que incluyen un gran número de datos estadísticos de gran valor técnico y ejecutivo, con información de la evolución de los troyanos bancarios frente al “malware” más tradicional, nuevas versiones de troyanos bancarios, porcentaje de detección de troyanos por unos 40 antivirus diferentes, familias de troyanos más detectadas, porcentaje de troyanos por familias y otros datos cualitativos y cuantitativos de interés.





Para una protección integral se recomienda la combinación de nuestros servicios antiphishing y antitroyanos.

ANTI-FRAUDE INTEGRAL

Hispasec ofrece un servicio 24x7 llamado AntiFraude Integral, que incluye Anti-Phishing y Anti-Troyanos, junto con herramientas opcionales como LogSecurityInspector o acceso al buzón abuse. De esta forma, y siempre con tiempos de respuesta excelentes, procuramos ampliar la seguridad de nuestros clientes contra los intentos de fraude por Internet.

Todos nuestros servicios están basados en procesos respetuosos de las normas de protección de datos y confidencialidad, y en el conocimiento acumulado del que disponemos en Hispasec sobre el comportamiento típico de los creadores de malware.

Hispasec Sistemas S.L.

Avda Juan López Peñalver 17
Edificio Centro de Empresas CEPTA
Parque Tecnológico de Andalucía
29590 Campanillas (Málaga)

Telf: (+34) 902 161 025

Fax: (+34) 952 028 694

Información General

info@hispasec.com

Comercial

comercial@hispasec.com

www.hispasec.com