Guía de supervivencia contra ciberatracos millonarios

pandasecurity.com

panda

Sobre PandaLabs

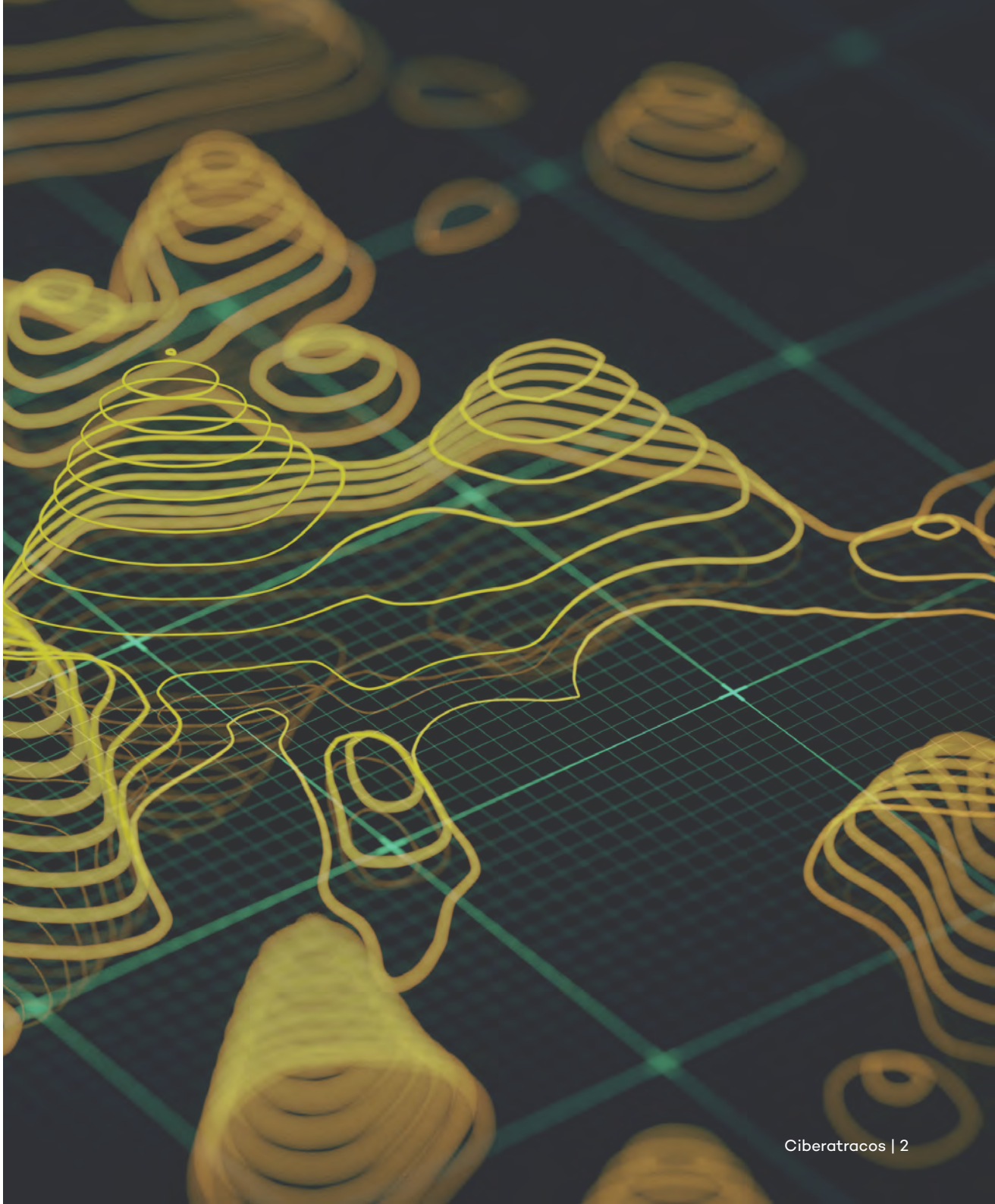
Pandalabs es el laboratorio antimalware de Panda Security y representa el centro neurálgico de la compañía en todo en cuanto al malware se refiere.

Desde el laboratorio se elaboran en tiempo real y de forma ininterrumpida las contramedidas necesarias para proteger a los clientes de Panda Security de todo tipo de códigos maliciosos a escala mundial.

Pandalabs se encarga asimismo de llevar a cabo el análisis detallado de todos los tipos de malware, con la finalidad de mejorar la protección ofrecida a los clientes de Panda Security, así como para informar al público en general.

Los técnicos del laboratorio mantienen un continuo estado de vigilancia, siguiendo muy de cerca las diferentes tendencias y evoluciones acontecidas en el campo del malware y la seguridad.

El objetivo es avisar y alertar sobre inminentes peligros y amenazas, así como formular previsiones de cara al futuro.



Principales conclusiones: ¿qué implican estos ataques?

Las amenazas han evolucionado, el malware es cada vez más sofisticado y las técnicas de ataque están también evolucionando: el objetivo ahora ya no es seleccionado al azar, los ataques son dirigidos, coordinados y utilizan diferentes vectores. El móvil tampoco es ya el mismo: desde el reconocimiento personal se ha pasado al lucro económico.

La ciberdelincuencia es un negocio muy rentable y atractivo. Los atacantes son hoy más profesionales, cuentan con más y mejores medios técnicos y económicos que les permiten hacer aún más sofisticados sus ataques. Este es el motivo por el que ya no temen ir directamente a por las propias entidades bancarias, algo impensable hace unos pocos años.

Para fortificar al máximo el sistema financiero la Unión Europea planea realizar por primera vez pruebas específicas de forma común para todo el marco europeo, similares a los tan comentados "test de estrés", para comprobar si los bancos cuentan con defensas suficientes contra los ataques cibernéticos más avanzados que se conocen. Asimismo, la ABE (Autoridad Bancaria Europea) quiere instaurar iniciativas adicionales para contrarrestar los efectos de un posible ataque a los sistemas digitales de la banca.

No hay que olvidar tampoco los ataques que tradicionalmente han acechado al sector financiero -aquellos que van dirigidos al cliente final del banco como el phishing o los troyanos bancarios- , y que siguen perpetrándose adaptándose a los nuevos tiempos como aquellos que utilizan malware para Android.

Introducción

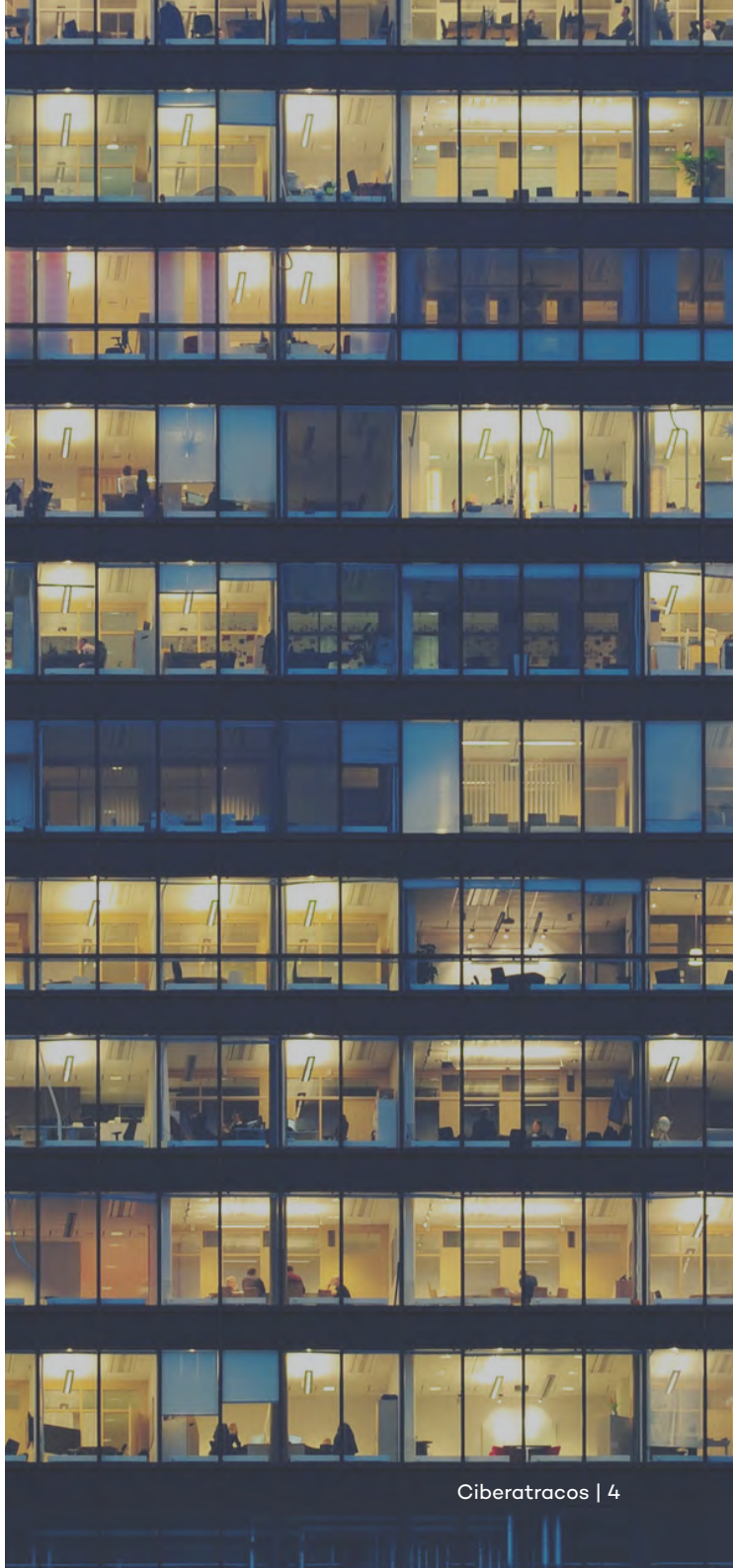
Durante años, conseguir dinero se ha convertido en el principal objetivo de los ciberdelincuentes, lo que ha puesto a los sistemas financieros en el punto de mira. Durante más de una década los ataques se han dirigido hacia el eslabón más débil de la cadena: el usuario final que utiliza servicios de banca online.

La innovación tecnológica se ha convertido en un medio para ofrecer el mejor servicio cómodo y de calidad a los clientes. Esta transparencia y acercamiento con el usuario a través de los servicios de banca online debe ir ligada a la prudencia financiera para lograr el éxito en el sector.

No obstante, esta estrategia supone algunas ventajas para los cibercriminales, como la escasa seguridad en el usuario final, el robo de cantidades pequeñas que pueden pasar desapercibidas durante cierto tiempo, etc... Sin embargo, también presenta ciertos inconvenientes principalmente relacionados con la necesidad de encontrar 'mulas' que trasporten el dinero, encontrar e infectar víctimas que utilicen alguno de los bancos atacados o evitar la acción de soluciones anti-malware.

La pregunta del millón es: ¿dónde están las grandes cantidades de dinero? Sin lugar a dudas, en las propias entidades financieras.

El cambio que se ha producido en los últimos años en la manera de actuar de los atacantes pone en relieve que explotan cualquier vulnerabilidad de los sistemas. **Una nueva etapa en el robo cibernético. Robo de dinero directamente de los bancos y no se sus clientes mediante ataques de phishing o emails inofensivos infectando ordenadores de los empleados de las instituciones bancarias.**



La táctica de atacar directamente a estas entidades puede reportar mucho dinero a los atacantes, pero también requiere de un gran esfuerzo y planificación por su parte. Penetrar en ellas es una tarea peliaguda y todavía resulta más complicado entender cómo funcionan sus sistemas internos para poder atacarlos, llevarse el botín y marcharse sin dejar huella. Se necesita una gran inversión para recopilar toda la información necesaria para este tipo de ataque. Aun así, parece merecer la pena si consigues llevarte un motín millonario en un sólo golpe.

Convertido en un blanco jugoso, no resulta sencillo para el sector financiero realizar funciones prioritarias como garantizar una asignación de recursos financieros de manera eficaz, contribuir al desarrollo y estabilidad monetaria del país o fomentar el ahorro y la inversión. Tampoco proteger los datos y cuentas de sus clientes.

A pesar de ser un ámbito que cuenta con las mejores soluciones contra el malware, tanto en el perímetro como en los dispositivos, **los ataques avanzados pueden comprometer cantidades ingentes de información sensible de la entidad.**

Legislación

El nuevo reglamento: GDPR

La legislación actual no está adaptada a los nuevos ciberdelitos ni a las nuevas necesidades, tanto tecnológicas como de gestión de la información. El Reglamento General de Protección de Datos (GDPR) de la Comisión Europea entra en vigor el 25 de mayo de 2018 y regulará la forma en que las empresas recopilan y procesan los datos personales de los residentes de toda la Unión Europea.

El impacto sobre el sector financiero será significativo ya que cualquier entidad, independientemente de su ubicación real, perteneciente a la UE y que utilice los datos personales de sus clientes para fines de marketing y ventas, estará sujeta a la GPR en menos de dos años. **Si una institución financiera no cumple la GDPR, podría ser sancionado con una multa de hasta 20 millones de euros o el 4 por ciento de su volumen de negocios anual internacional.**

La falta de conocimiento de la norma por parte de los equipos de IT podría resultar muy costosa para los bancos que dejen la implementación de sus estrategias de GDPR para el último minuto. Limpiar la base de datos personales después de un periodo de tiempo determinados, reportar un incidente de seguridad en las 72h siguientes al ataque a todos los afectados así como actualizar la estrategia de seguridad, son puntos clave dentro de la nueva legislación.

Los sistemas financieros están expuestos a riesgos que requieren esfuerzos consistentes para operar de forma segura. Teniendo en mente que uno de los mayores problemas a los que se enfrenta el sector financiero hoy en día es la protección de los datos personales ante una infracción de seguridad, debe existir un protocolo a seguir en caso de ciberataque. La GDPR exige transparencia; alinear los procesos existentes con ella más temprano que tarde va a actualizar las medidas de seguridad y garantizar que las operaciones de negocio son compatibles con el nuevo reglamento.

Afectará a las empresas con **datos personales de personas físicas miembros de la UE.**

Entrará en vigor a partir del **25 de mayo de 2018.**

Se aplicará al tratamiento de datos personales de **personas físicas dentro de la UE.**

Migración a Cloud

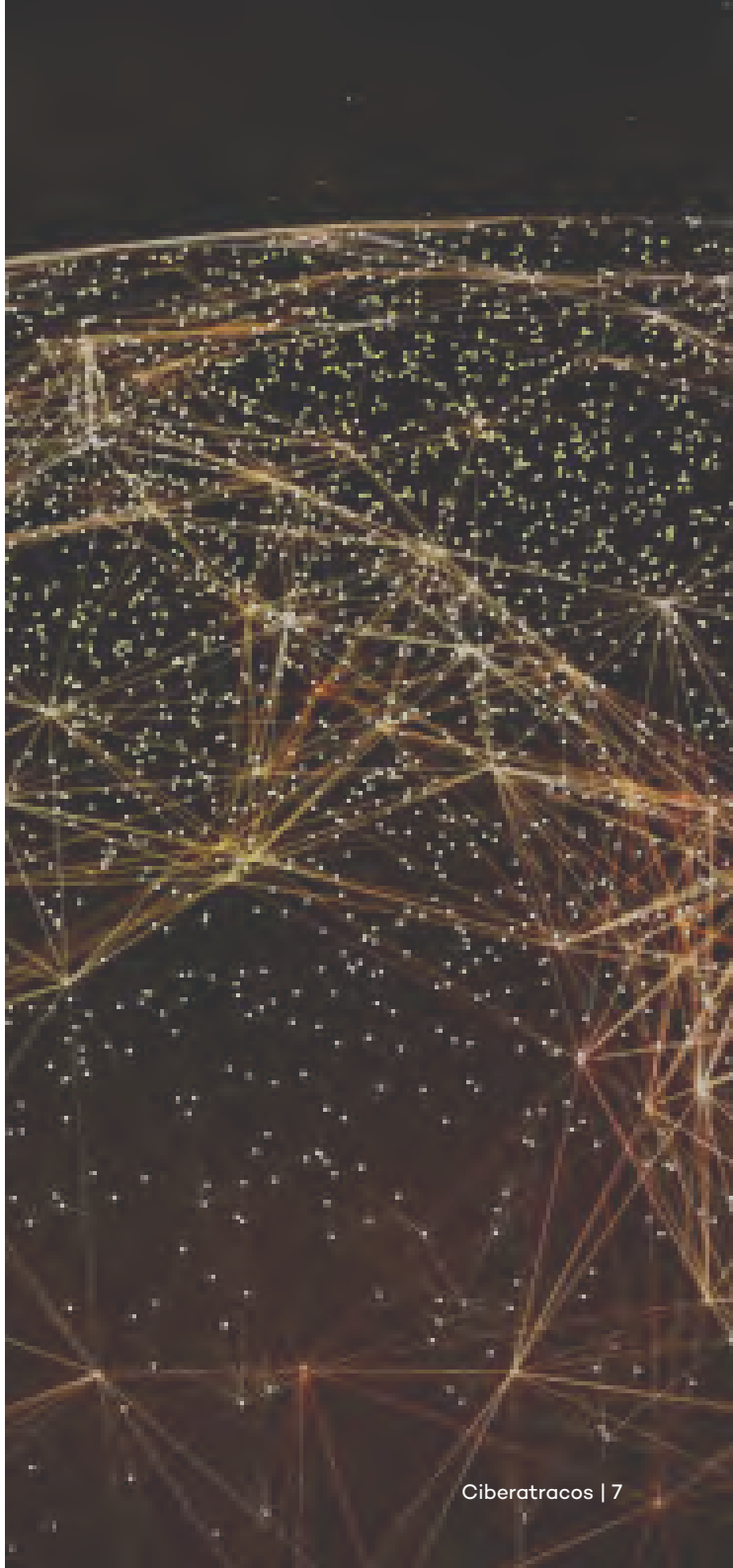
El sector financiero es un complejo conjunto de varios jugadores regulado desde varios ángulos diferentes. Hay que tener en cuenta tanto la cobertura de seguridad de las redes y de la información estipulada en diferentes normativas como la NIST (National Institute of Standards and Technology) así como las obligaciones en el panorama normativo europeo (tanto a nivel de la Unión Europea como de los Estados Miembros).

El Cloud Computing se está adoptando gradualmente dentro del sector financiero europeo. Sin embargo, el proceso de migración a la nube no está todavía maduro. A pesar de que las instituciones financieras y las autoridades supervisoras parecen tener una visión clara de los beneficios económicos y técnicos relacionados con la implementación de la nube, tanto pública como privada, son cautelosos acerca del riesgo de perder el control sobre los activos de información y la mayoría todavía dependen de una infraestructura propia.

Uno de los principales inhibidores en la adopción del cloud está basado en los argumentos del Banco Central Europeo y los correspondientes Bancos Nacionales y normativas como la NITS, ya que estos organismos están obligados a un control riguroso de ubicación de sus datos y trazabilidad del servicio cuando son datos clasificados como secretos y/o confidenciales.

A pesar de que el enfoque más común utilizado por las instituciones financieras es un híbrido de nubes privadas y públicas, la normativa establece que cuando se traten datos críticos para el negocio se requiere la utilización de una Cloud privada. Este mecanismo se considera, en general, más apropiado y es favorecida por las autoridades de supervisión financiera nacional, ya que proporciona un mayor control sobre los datos y operaciones.

La falta de directrices formales para servicios basados en la nube y la falta de madurez de los procesos de evaluación está bloqueando la adopción del Cloud Computing como facilitador para la innovación y ampliamente defendido como tal por la Comisión Europea en el mercado único Digital.



Ciberatracos millonarios

Cuando los ciberdelincuentes comenzaron a fijarse en el sector financiero, tuvieron claro que su principal objetivo tenía que ser el cliente porque contaba con menos medidas de seguridad y, de forma relativamente sencilla, podían robar su identidad para hacerse pasar por él ante su banco. El cliente era el eslabón débil de la cadena.

Sin embargo, en los últimos 2 años han aparecido grupos sofisticados –y ambiciosos- que han ido un paso más allá y cuyo objetivo es infiltrarse en las propias entidades para llevar a cabo atracos millonarios.

Bangladesh Bank

Uno de los mejores ejemplos fue el sufrido por el Banco Central de Bangladesh en febrero de 2016, cuando un grupo de atacantes consiguió infectar el sistema con malware creado específicamente para la ocasión e intentó realizar transferencias fraudulentas por un valor de 951 millones de dólares. Dicha cantidad de dinero se encontraba en la cuenta que el Banco Central de Bangladesh tenía en el Banco de la Reserva Federal de Nueva York. Afortunadamente, la mayoría de trasferencias pudieron ser bloqueadas y 'únicamente' se robaron 81 millones de dólares. Pero este no es el único caso.

Tien Phong Bank

Tien Phon Bank, un banco comercial vietnamita, sufrió un ataque similar en el último trimestre de 2015. En dicha ocasión los ciberdelincuentes también trataron de realizar transferencias a través de SWIFT pero la entidad se dio cuenta a tiempo y logró bloquear las transferencias que ascendían a 1 millón de dólares.

Banco del Austro

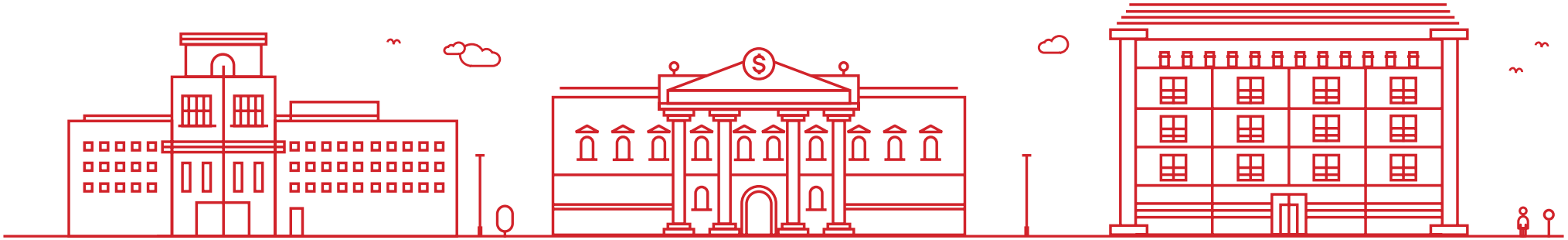
Unos pocos meses antes, en enero de 2015, un banco ecuatoriano –Banco del Austro– sufrió un ataque parecido y le lograron robar 9 millones de dólares.

.

Bangladesh Bank
Bangladesh → **$81 mm**

Banco del Austro
Ecuador → **$9 mm**

Tien Phong Bank
Vietnam → **$1 mm**



En todos ellos se utilizó malware para llevar a cabo el ataque y las transferencias de dinero fueron realizadas a través de la red SWIFT (Sociedad para las Comunicaciones Interbancarias y Financieras Mundiales). Un posible ataque a esta red sería la mayor preocupación, ya que la plataforma SWIFT es utilizada por la mayoría de entidades financieras mundiales para realizar transferencias bancarias en un entorno seguro y si resultase vulnerable ante un ataque externo todo el sistema estaría en peligro. Afortunadamente, parece que este no ha sido el caso y SWIFT publicó una nota de prensa en la que afirma claramente lo siguiente: "Ni la red, ni los servicios centrales de mensajería, ni el software de SWIFT se han visto comprometidos."

Sin embargo, esto depende del punto de vista: los ciberdelincuentes han logrado utilizar la red SWIFT para perpetrar estos atracos. Y para ello han ido de nuevo a por el eslabón más débil de la cadena. SWIFT proporciona un entorno seguro, pero al final cada institución financiera tiene su propio sistema interno que debe comunicarse con esta red. Del mismo modo que los ciberdelincuentes van a por los clientes finales de los bancos con troyanos bancarios, ahora en lugar de ir a por la red SWIFT van tras las entidades que se conectan a ella.

Estos 3 casos han sido perpetrados por el mismo grupo, y actualmente hay evidencias que apuntan a que Corea del Norte estaba detrás de estos ataques. En diciembre de 2016 se dio a conocer que SWIFT había alertado a sus clientes, ya que se estaban dando nuevos casos de ataques. Según declaraciones a Reuters de Stephen Gilderdale, responsable del Programa de Seguridad de Clientes en SWIFT, bancos utilizando la red SWIFT -tanto bancos centrales como bancos comerciales-, han sido atacados un número significativo de ocasiones desde el robo al Banco Central de Bangladesh. **Un 20% de estos ataques han conseguido robar fondos.**

Otra táctica que está en boga hoy en día es atacar los TPV (Terminales de Punto de Venta) para robar la información de las tarjetas de crédito y débito que sean utilizadas en dichos terminales. En el análisis que hicimos de la industria hotelera ya pudimos ver cómo la mayoría de los ataques que sufría este sector era a través de malware que infecta los TPV y roba los datos de las tarjetas utilizadas por los clientes en sus establecimientos. Pero esta es una práctica que afecta a todo tipo de comercios, desde grandes cadenas de supermercados a restaurantes.

En PandaLabs hemos analizado diferentes ataques llevados a cabo con malware diseñado para este trabajo, como el caso del PunkeyPOS donde los atacantes habían comprometido establecimientos a lo ancho y largo de Estados Unidos.

TPVs infectados por PunkeyPOS

Podéis encontrar información de otras familias de malware diseñado para infectar TPVs- como Multigrain o PosCardStealer- en el Media Center de Panda Security.

Tendencias de la actividad en ciberdelincuencia financiera

Los primeros ataques al sector financiero surgieron en el año 2003. En aquel entonces la banca online estaba popularizándose y el número de operaciones realizadas por sus clientes a través de Internet se multiplicaba rápidamente. Las medidas utilizadas por las entidades financieras para identificar a sus clientes eran muy básicas: simplemente con el usuario y contraseña podías tener acceso a toda tu información y realizar todo tipo de operaciones.

Es aquí cuando surgieron los primeros ataques en forma de **phishing, correos electrónicos que simulan provenir de entidades bancarias** indicando que hay algún problema de seguridad con tus credenciales y que te suspenderán la cuenta hasta que vayas a la página web que te indicaban. Al pinchar en el enlace proporcionado lleva a páginas web falsificadas. De esta manera, el usuario, creyendo estar en un sitio de toda confianza, introduce la información solicitada que, en realidad, va a parar a manos del estafador.

Algo más de un año después comenzaron a aparecer los primeros **troyanos bancarios,** cuya finalidad era la misma que en el caso del phishing: robar la identidad de la víctima para engañar al banco y sustraer todo el dinero de las cuentas. Las entidades bancarias han reaccionado ante la amenaza que suponen los troyanos bancarios y han mejorado sensiblemente la seguridad y la autenticación de los clientes. Pero también las amenazas se han sofisticado, apareciendo troyanos que tratan de evadir todas las técnicas de protección.

Las técnicas que utilizan para robar la información han ido mejorando a medida que los bancos, conscientes de la amenaza que suponen estos troyanos, han aumentado las medidas de seguridad en sus páginas web. Por ejemplo, la implantación de los teclados virtuales para el registro de los usuarios, supuso un importante avance en la seguridad de estas páginas web. De esta manera, un **keylogger** no podría capturar los datos introducidos por el usuario.

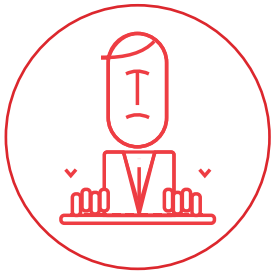
Sin embargo, los creadores de malware desarrollaron nuevas funcionalidades para los troyanos bancarios, haciéndoles capaces de registrar los movimientos realizados con el ratón e incluso realizar capturas de pantalla o de vídeo, como es el caso de Trj/Banbra.DCY.

Phishing

Crea una url falsa para obtener tus datos y suplantar tu identidad

Troyanos Bancarios

Instala varias aplicaciones para que los hackers controlen tu equipo y roben tu información.



Keylogger

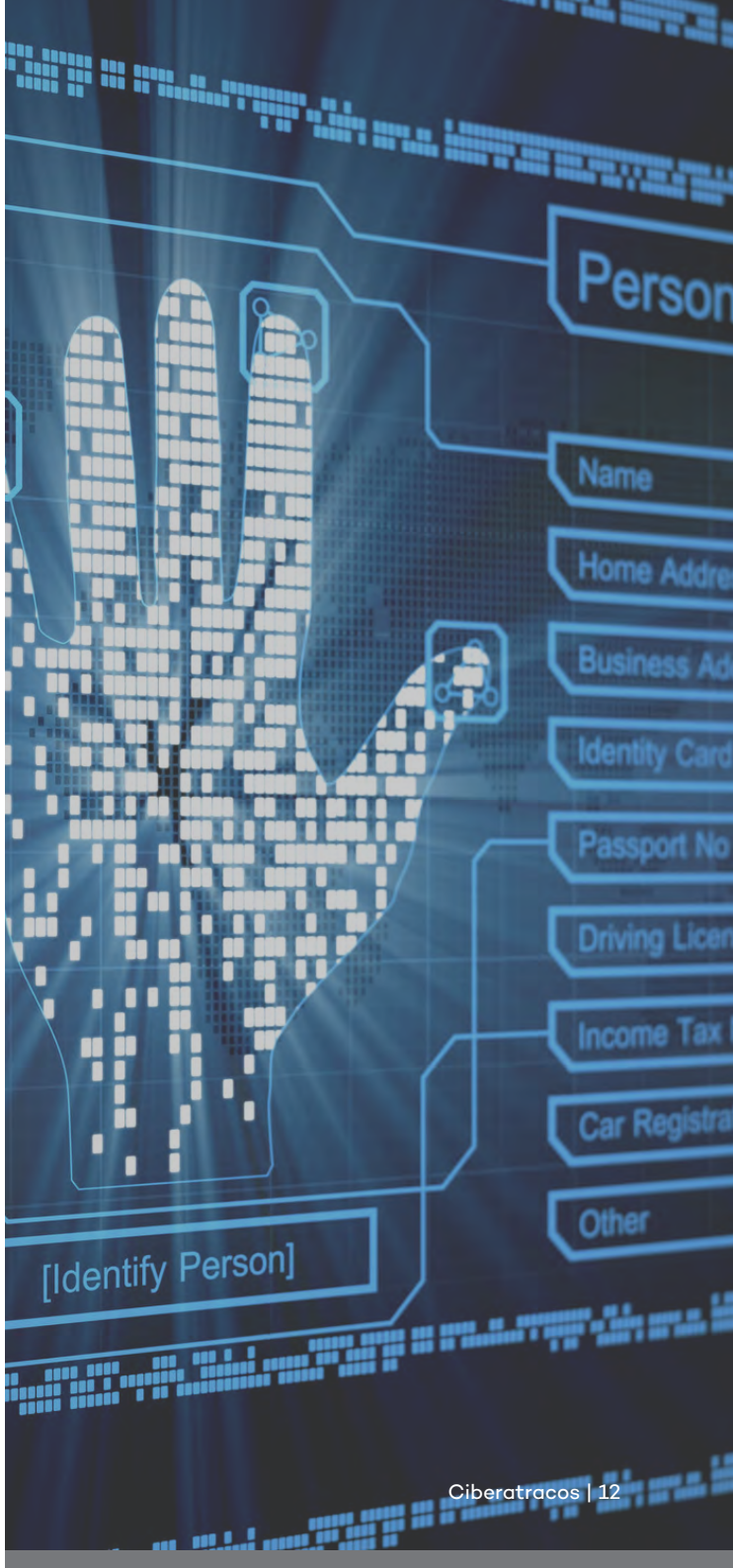
Recoge, guarda y envía todas las pulsaciones realizadas por el usuario.

Algunos ejemplares, como los pertenecientes a la familia BankoLimb, tienen un archivo con una lista de URLs de bancos objetivo. Cuando el usuario infectado con un BankoLimb accede a alguna página web cuya dirección coincida con la de su lista, el troyano se activará e inyectará código html extra en la página del banco. Esto implica que, además de los campos habituales que tiene que rellenar el usuario para registrarse, tendrá que proporcionar información adicional. El usuario está en la página legítima, pero ligeramente modificada. Por eso **es importante que si un usuario está navegando, accede a la página de su banco y le solicitan más información de la habitual, no confíe y no introduzca ningún dato en dicha página, porque posiblemente su ordenador esté infectado con algún troyano bancario** y toda la información que introduzca será capturada.

Otras veces, los troyanos superponen la página falsa sobre la original para que el usuario no se dé cuenta o directamente redirigen al usuario a una página falsa que imita a la original. Una vez que el usuario se registre en dicha página falsa puede mostrar una página de error o incluso podría redirigir al usuario de nuevo a la página original del banco para evitar que el usuario sospeche. Algunas variantes de la familia del troyano Sinowal eran realmente sofisticadas, siendo capaces de modificar datos "on the fly", es decir, al vuelo. Por ejemplo, si un usuario está realizando una transferencia a través de la página web de su banco, estas variantes pueden modificar los datos del receptor de dicha transferencia una vez enviada la petición. Además el resultado que se le devuelve al usuario sería con los datos originales, por lo que el usuario no se daría cuenta de la estafa.

Otras variantes consultan al servidor para saber si deben realizar alguna acción en función de las páginas que el usuario está visitando. De esta forma no depende de un fichero de configuración y el ciberdelincuente puede ampliar o modificar la lista de sitios web de las que quiere robar información, inyectar código, etc.

Cada vez más habitual que accedamos a la banca online a través de nuestro smartphone, por lo que cada vez se crea más malware para Android cuyo objetivo es el mismo que el malware bancario de PC. Un smartphone no deja de ser un ordenador con su sistema operativo, aplicaciones, etc. y existen ya miles de variantes de troyanos bancarios para estos dispositivos.



La cantidad de familias de malware bancario a lo largo de la historia es realmente numerosa. Por simplificar las podríamos dividir en dos ramas principales:

1. Brasileña

(Banbra, Banker, Bancos, etc.)

Sus objetivos son clientes de entidades brasileñas, de América del Sur y en ocasiones de España y Portugal. Tecnológicamente no son los más destacados pero sí que son los más creativos a la hora de diseñar técnicas de ingeniería social para engañar a sus víctimas.

2. Rusa

(Bankolimb, Zeus, Sinowal, SpyEye, Citadel, Dyreza, etc.)

Sus objetivos son principalmente clientes de entidades bancarias europeas y norteamericanas. Históricamente han sido –y son- los más sofisticados a nivel técnico.

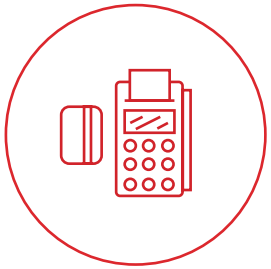
Muchos de ellos tienen bastante parecido ya que en su día se publicó el código fuente de Zeus, y a raíz de él surgieron multitud de subfamilias basadas en él: SpyEye, Citadel, Ice IX, Ramnit, Zberp, Kins, Murofet, GameOver (Zeus P2P), etc.

Tradicionalmente las víctimas de estos ataques han sido siempre los clientes de entidades financieras, al ser el punto más débil de la cadena y el que más sencillo resulta comprometer.

Sin embargo en los últimos dos años hemos visto cómo los grupos de delincuentes han diversificado, y buscan dinero en otros ámbitos:

TPVs

Terminales de Punto de Venta, controlados por ordenador. Existe malware creado específicamente para este tipo de terminales, lo que permite robar la información de todas las tarjetas utilizadas en estos terminales. Esto posibilita el robo de datos de miles de tarjetas de crédito y débito por cada terminal, afectando a todo tipo de comercios (restaurantes, hoteles, supermercados, etc.)



Cajeros automáticos

No dejan de ser ordenadores, y ya se han visto casos donde los delincuentes los han infectado para obtener dinero directamente. Esto lo pueden conseguir mediante la manipulación directa del cajero (instalando skimmers que copian las tarjetas utilizadas en el cajero), o bien comprometiendo la red interna del banco y desde allí accediendo a los cajeros.

Bancos

¿Quién tiene más dinero que ninguna otra víctima? Los propios bancos. Estos ataques son muy sofisticados y necesitan de recursos y mucho tiempo de planificación, pero pueden llegar a robar cientos de millones de dólares en un solo golpe.

Recomendaciones para evitar ciberatracos

Una de las cosas más frustrantes por las que pasan las víctimas de un ataque es la falta de información sobre el mismo. Por ejemplo, tras el ataque al Banco Central de Bangladesh se consiguieron recuperar tres ejemplares de malware, pero eso fue todo lo que quedó. Seguramente los atacantes emplearon muchas otras herramientas que fueron eliminadas y de las que las víctimas no sabrán nunca nada.

El conocimiento es poder y saber cómo ha sucedido un incidente ayudará a resolver cualquier fallo de seguridad o vulnerabilidad del entorno. Tener una visibilidad ilimitada de todo lo que sucede en tu parque informático te permite tener un control absoluto y evitar potenciales ataques antes de que se produzcan.

La inexistencia de un ciberespacio común, las normas, certificaciones, la interoperabilidad y la seguridad jurídica son algunos de los principales obstáculos a la hora de la adopción del sistema Cloud Computing en la banca. Un sistema que permite a las entidades financieras obtener beneficios como la reducción de costos de software, un mejor rendimiento del equipo, el aumento de la fiabilidad de los datos o el acceso universal a los documentos; entre otros.

Entonces, ¿cómo debe tratar la información nuestro software de ciberseguridad alojado en Cloud para actuar de forma eficaz y en cumplimiento de la normativa?

Información clasificada como Secreta: el servicio no debe acceder a información personal clasificada como Nivel Alto por la LOPD o clasificada como secreta para la Entidad Financiera. El único matiz se podría dar en que, como parte del servicio, se recoja, de forma indirecta, información de uso de los recursos IT de la compañía por parte de los usuarios y quizá esta información esté recogida como una restricción en el reglamento interno de conducta, pudiendo darse el caso, que los operadores de la protección, personal de la Entidad Financiera, pueda conocer esta información a partir de los datos del servicio.

Información clasificada como Confidencial: el servicio accede a información de usuarios clasificada como Nivel Básico por la LOPD. Esta información será el login del usuario, nunca la password (esta nunca se recoge), el nombre de la máquina, si identifica unívocamente al usuario y la dirección IP del equipos, si igualmente identifica unívocamente a un usuario. Estos datos son necesarios para la correcta prestación del servicio y por tanto entendemos que los operadores podrían ser autorizados para acceder a dichos datos.

Estas dos características son en las que se sustenta el modelo de seguridad de Adaptive Defense 360, el primer servicio de ciberseguridad avanzada que ofrece una

panda

protección de última generación (NG EPP) y tecnologías de detección y remediación (EDR), con la capacidad de clasificar el 100% de los procesos en ejecución.

De esta manera, **la entidad financiera podrá proteger su principal activo, los datos e información sensible de sus clientes, con una solución capaz de detectar una fuga de información tanto si viene del malware como de sus empleados, uno de los aspectos más valorados en el sector.** Adaptive Defense 360 obtiene datos enriquecidos del sistema SIEM permitiendo tener una visibilidad total de cada endpoint en el puesto de trabajo.

Además de cumplir la exigente legislación vigente del sector y sus funciones de detección y bloqueo de cualquier ataque dirigido al sistema, **Adaptive Defense 360** permite descubrir y solucionar vulnerabilidades en los sistemas y aplicaciones y prevenir el uso de programas no deseados como barras de navegadores, adware o add-ons.

La solución corporativa de Panda Security forma parte de una plataforma que utiliza la lógica contextual que analiza, categoriza y correlaciona los datos que obtiene sobre las ciberamenazas para llevar a cabo tareas de prevención, detección, respuesta y remediación.

Una solución de ciberseguridad avanzada avalada por AV- Comparatives y por la garantía de todos los productos de Panda Security. **Reinventamos la ciberseguridad.**

Adaptive Defense 360

Contacta con nosotros para más información

ARGENTINA
+54 11 6632 6632
argentina@pandasecurity.com

BOLIVIA
+59 12 21 20 300
bolivia@pandasecurity.com

BRASIL
+55 11 3054-1722
brazil@pandasecurity.com

CHILE
+56 2 6394774
chile@pandasecurity.com

COLOMBIA
+57 1 2560344
colombia@pandasecurity.com

COSTA RICA
+506 2523-4300
ventas@cr.pandasecurity.com

ECUADOR
+593 02 6012384
ecuador@pandasecurity.com

EL SALVADOR
+503 22087435
ventas.elsalvador@pandasecurity.com

GUATEMALA
+502 66400100
ventas.guatemala@pandasecurity.com

MÉXICO
+52 55 8000 2381
mexico@pandasecurity.com

PANAMÁ
+507 833 7263
ventas.panama@pandasecurity.com

PARAGUAY
+595 21 6075 94
paraguay@pandasecurity.com

PERÚ
+51 1 204 55 00
peru@pandasecurity.com

URUGUAY
+598 2 402 0673
ventas@uy.pandasecurity.com

VENEZUELA
+58 212-7612535
venezuela@pandasecurity.com

Adaptive Defense 360

Visibilidad sin Límites, Control Absoluto

pandasecurity.com

panda