Identificación de prácticas fraudulentas típicas

c Secure Bank

Porqué Group-IB

Group-IB — Una de las principales compañías internacionales para la prevención e investigación de "cibercrimen y fraude" utilizando altas tecnologías

EUROPOL INTERPOL

Socio oficial
EUROPOL y INTERPOL

OSCE

Recomendado por la Organización para la Seguridad y la Cooperación en Europa (OSCE)

WORLD ECONOMIC FORUM

Miembro permanente del Foro Económico Mundial

1000+

investigaciones exitosas en todo el mundo, de 150 casos penales particularmente complejos

$300 millones

devuelto a clientes del Group-IB debido a nuestro trabajo

Forrester Gartner

Inteligencia de amenazas del Group-IB –
entre los mejores sistemas mundiales según la evaluación de Forrester y Gartner

BUSINESS INSIDER

Una de las 7 empresas más influyentes en el campo de la ciberseguridad según Business Insider

IDC

Líder del mercado ruso en investigación cibernética

Sobre nosotros comentan:

theguardian Bloomberg Forbes REUTERS Esquire

ПЕРВЫЙ КАНАЛ РОССИЙСКАЯ ГАЗЕТА ИЗВЕСТИЯ ВЕДОМОСТИ РОССИЯ 1 Коммерсантъ

Historia de la empresa

2003 — Año de fundación del Grupo-IB

2009 — Entra en el mercado internacional

2010 — El Laboratorio de criminalística computarizada GIB se convirtió en el **más grande de Europa del Este**

2011 — Es creado CERT-GIB - un centro de **respuesta las 24 horas** en incidentes IB

2012 — Se creó el sistema **Inteligencia de amenazas**

2014 — Salió al mercado el primer producto del Group-IB basado en el sistema Inteligencia de amenazas: detector de amenazas en la red corporativa. **TDS**

2015 — Se han desarrollado sistemas para la **detección temprana de fraude** para sistemas de pago y recursos de Internet

2016 — Se presenta una solución para proteger contra el código malicioso previamente desconocido **TDS Polygon**, basado en tecnologías de aprendizaje automático.

2017 — Trabajo activo en mercados internacionales, **apertura de oficinas en el exterior**

GROUP-IB

Los muchos años de experiencia de Group-IB se materializa en el sistema de detección temprana de amenazas cibernéticas: una línea de productos de alta tecnología basada en los datos más actualizados y un análisis en profundidad de los verdaderos ataques de hackers.

260+
empleados

40%
desarrolladores

27
edad promedio

45 000
horas de respuesta

Base de recursos única

Una base de recursos única, acumulada durante 15 años de operación

Hemos creado una infraestructura de alta tecnología para controlar la actividad de piratas informáticos, rastrear redes de bots y extraer los datos necesarios para evitar incidentes. El 90% de los datos entran al sistema desde fuentes cerradas, la mayoría absoluta de ellos es única. Controlamos sitios cerrados, monitoreamos cambios en botnets, extrayendo archivos de configuración de programas maliciosos y la información sobre identificadores robados.

1 INFRAESTRUCTURA DE RED

- Red de monitoreo distribuida y trampas - HoneyNet
- Análisis de botnets
- Rastreadores de ataques de red
- Monitoreo de foros de hackers y comunidades cerradas en red
- Datos del sensor TDS

2 HUMAN INTELLIGENCE

- Resultados de los exámenes de criminalística del Laboratorio Group-IB
- Materiales de investigación
- Monitoreo y análisis de software malicioso
- Base de datos de quejas y la práctica de responder a incidentes CERT-GIB
- Resultados de auditoría
- Análisis de Target Group-IB

3 INTERCAMBIO DE DATOS

- Equipos de respuesta CERT
- Registradores y proveedores de hosting
- Fabricantes de equipos de protección
- Organizaciones y asociaciones para contrarrestar las amenazas cibernéticas
- Europol, Interpol y las agencias policiales

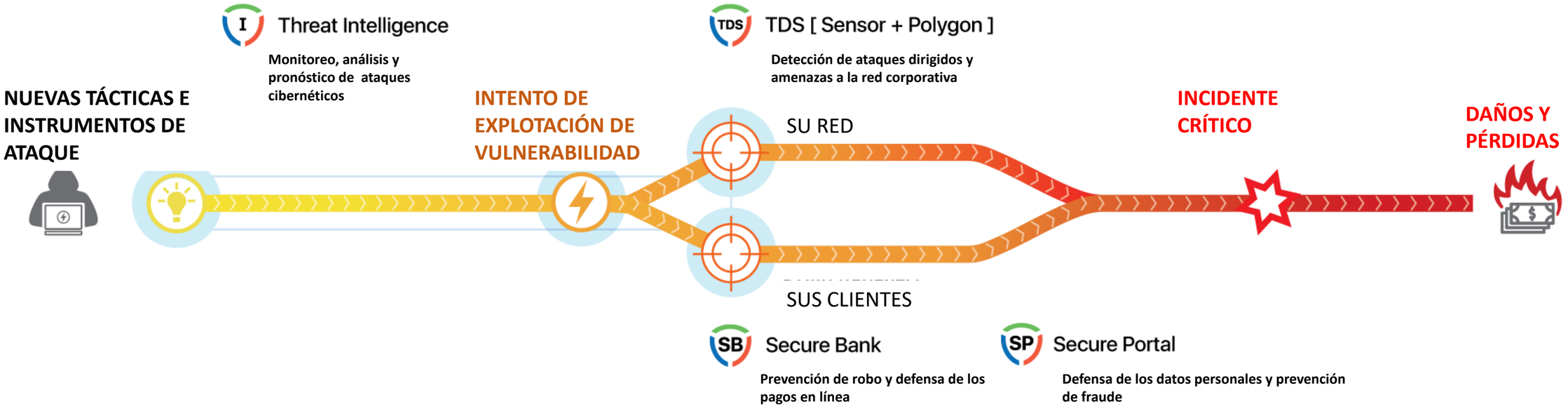
Sistema de alerta temprana para ciberamenazas

Le damos lo más importante: el tiempo para prepararse para los incidentes.

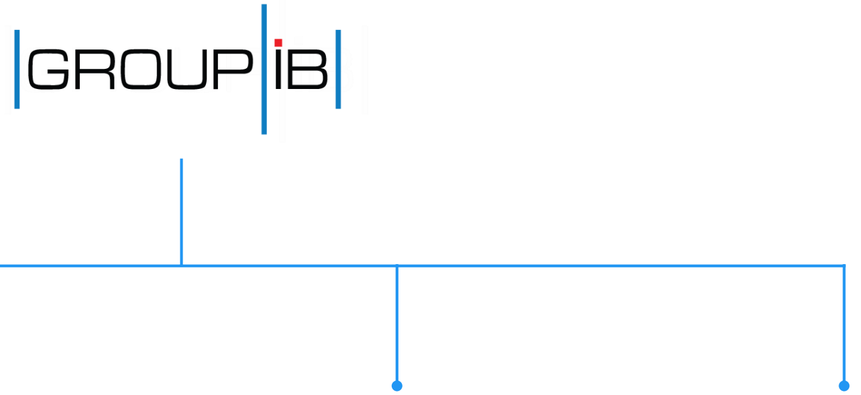
El sistema de alerta temprana de amenazas cibernéticas del Group-IB le permite saber rápidamente sobre nuevas amenazas y bloquear su aparición en sus líneas de defensa. Se basa en la experiencia de 15 años de nuestro equipo, el análisis en profundidad de las campañas de hackers y los datos de inteligencia actual del mundo del cibercrimen.

15 años

experiencia en el campo de criminalística computarizada, consultoría y auditoría de seguridad de la información



Estructura de la compañía



SISTEMA DE ALERTA TEMPRANA

- Inteligencia de amenazas
- TDS
- Banco seguro
- Portal seguro

PREVENCIÓN DE AMENAZAS

- Auditoria de seguridad
- Evaluación de compromiso
- Red Teaming
- Protección de marcas
- Anti piratería

RESPUESTA 24/7/365

- Centro de respuesta para incidentes de seguridad de la información CERT-GIB

INVESTIGACIÓN DE INCIDENTES

- Informática criminalística e investigación de código malicioso
- Investigación de incidentes de IS
- Investigaciones financieras y corporativas independientes

Las direcciones de productos y servicios del Grupo-IB se complementan entre sí, lo que permite lograr un efecto sinérgico en la lucha contra diversos tipos de amenazas..

Group-IB & AIG CyberEdge

El primer producto combinado en Rusia de protección y aseguramiento contra el delito cibernético

En algunos casos, los cibercriminales usan no solo programas maliciosos, sino también ingeniería social, engaño y soborno de empleados. Gracias a nuestra cooperación con AIG, los clientes de Group-IB también están protegidos contra estos ataques complejos.

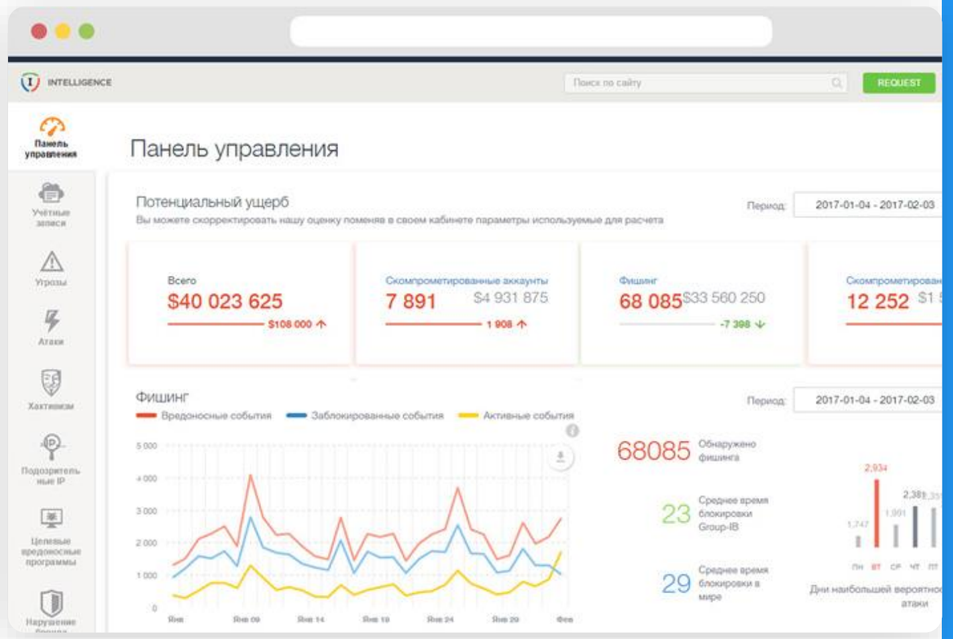
QUÉ CUBRE EL SEGURO

- Pérdidas debido a violaciones de datos
- Investigación administrativa de los datos
- Costos de respuesta en cas de violaciones de datos

Inteligencia de amenazas

Monitoreo, análisis y previsión de amenazas para la empresa, clientes y socios

- Información estratégica para una evaluación de riesgos equilibrada y priorización de amenazas
- Datos operativos para prepararse para ataques y configuraciones de seguridad
- Indicadores tácticos que minimizan el tiempo de respuesta a un incidente



Incluido en el registro de software nacional

Forrester Gartner IDC

Group-IB — uno de los mejores proveedores de Inteligencia de amenazas en el mundo por la evaluación de las agencias analíticas Gartner (2015) y Forrester (2017). En 2017, la agencia IDC reconoció al Grupo IB como líder del mercado en el estudio de las amenazas cibernéticas

GROUP-IB

- Notificación operacional de ataques y amenazas
- Interfaz web visible
- Seguimiento, análisis y predicción de actividad de hackers en industrias interesantes
- Soporte para STIX / TAXII en el suministro de datos de amenazas
- Acceso directo a datos comprometidos e identificadores
- Asistencia las 24 horas

Resultados de uso de Inteligencia de amenazas

Analistas y equipos de respuesta a incidentes

Priorización cualitativa de incidentes, según los datos de Inteligencia de amenazas

Aceleración de procesos de respuesta a incidentes

Inmersión en el contexto detallado de amenazas, conocimiento de tácticas y herramientas de grupos delictivos potencialmente interesados en la empresa

CEO y alta dirección

Maximizar el ROI de la inversión en sistemas de seguridad, equipos y analistas de respuesta a incidentes

Obtener información sobre las amenazas que afectan las decisiones de gestión

Evitar el uso de la marca de la compañía con fines delictivos, reduciendo los riesgos para la reputación

CISO

- Desarrollar una estrategia de IB basada en una comprensión profunda de la evolución de las amenazas cibernéticas y analizar los ataques reales en su sector
- Una elección ponderada de soluciones tecnológicas: para protegerse de las amenazas actuales
- Aumento de la eficiencia y las capacidades de los analistas y los equipos de respuesta a incidentes

MSSP

- Brindar a los clientes un servicio basado en una comprensión profunda del contexto de las amenazas
- Mejor orientación de propuestas para clientes basadas en datos sobre las amenazas reales para ellos
- Pronosticar el desarrollo de amenazas y sus contramedidas basadas en datos globales de Inteligencia de amenazas

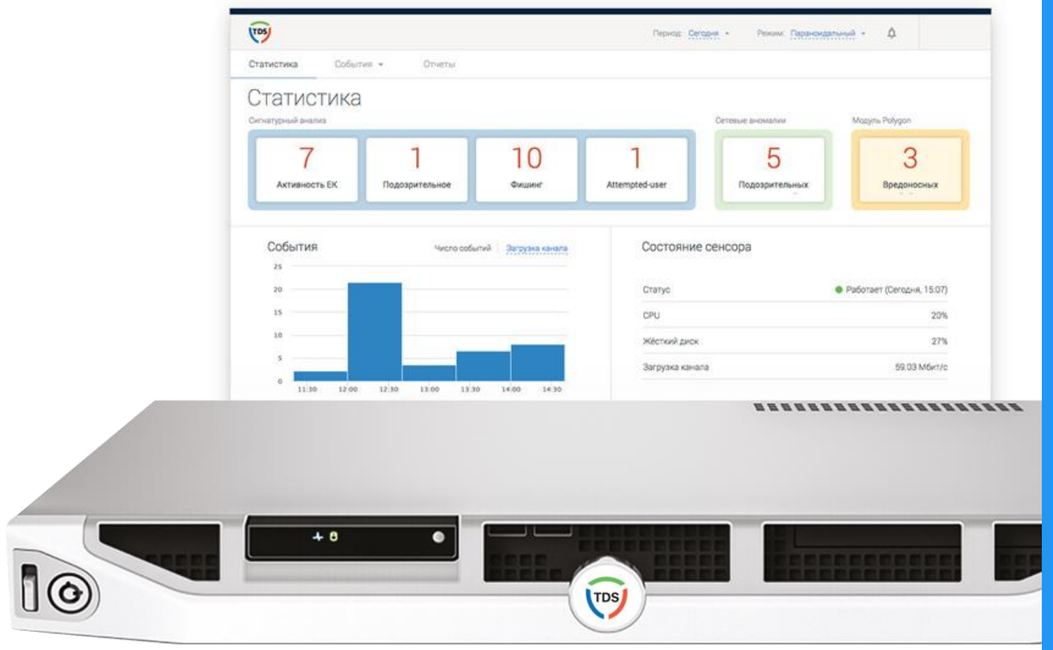
Inteligencia de amenazas del Group-IB le permitirá:

- Reducir el tiempo de respuesta a los incidentes a un mínimo
- Seguir la aparición de nuevas herramientas y métodos de ataque
- Obtener datos personalizados de sitios cerrados de piratas informáticos
- Evaluar la efectividad de la estrategia de inversión elegida en la seguridad de la información de la empresa

Sensor TDS

TDS — detección de ataques selectivos

Detecta nodos infectados, evita intrusiones, fugas, ataques selectivos y espionaje industrial



Gracias a un profundo conocimiento de los detalles de los ataques selectivos y la actividad de grupos delictivos en diferentes regiones del mundo, identificamos amenazas que son imperceptibles para otros, que incluyen:

- interacción de red no deseada y peligrosa
- objetos peligrosos transferidos
- Programas espiones
- herramientas de gestión remota
- Intención de explotar vulnerabilidades

Fuentes únicas y autoría para la detección de amenazas de alta precisión:

1. Algoritmos de análisis de comportamiento + aprendizaje automático
2. Información sobre ataques del Laboratorio de criminalística informática Forense
3. Datos del sistema Inteligencia de amenazas del Grupo-IB

GROUP-IB

- Notificaciones instantáneas de todos los tipos de programas maliciosos actuales y desconocidos previamente
- Detección de dispositivos móviles infectados en redes Wi-Fi
- Soporte y asesoramiento las 24 horas
- Interfaz web amigable para el usuario e informes visuales
- Análisis de registro manual y detección de incidentes críticos por los especialistas de Group-IB
- Clasificador actualizado periódicamente para detectar el grado de peligro de los objetos

Detector de amenazas en la red corporativa Polygon

Polygon lanza archivos recibidos de TDS en un entorno seguro y aislado dentro de su lazo de seguridad, analiza su comportamiento y llega a una conclusión objetiva sobre el grado de peligro del objeto

TDS Sensor + TDS Polygon

Granja de máquinas virulentas

Los archivos sospechosos se lanzan en un entorno de prueba que se puede personalizar según los detalles de su empresa y región.

Monitor de sistema de bajo nivel "Clasificador" actualizado regularmente

Sin revelar su presencia, el polígono en el nivel más bajo rastrea el comportamiento de los objetos cuando se inicia en un entorno seguro

El peligro del objeto se determina con la ayuda de Machine Mind y recibiendo nueva información con la regularidad especificada del clasificador.

Archivos adjuntos de correo
Archivos maliciosos recibidos como resultado de la aplicación de Ingeniería social

Archivos descargables:
objetos descargados por los usuarios y / o sus computadoras en segundo plano

Ataques dirigidos:
software malintencionados dirigido exclusivamente a su infraestructura

Otros:
Objetos maliciosos desconocidos anteriormente no detectados por los antivirus y otras señales.

Cómo funciona TDS

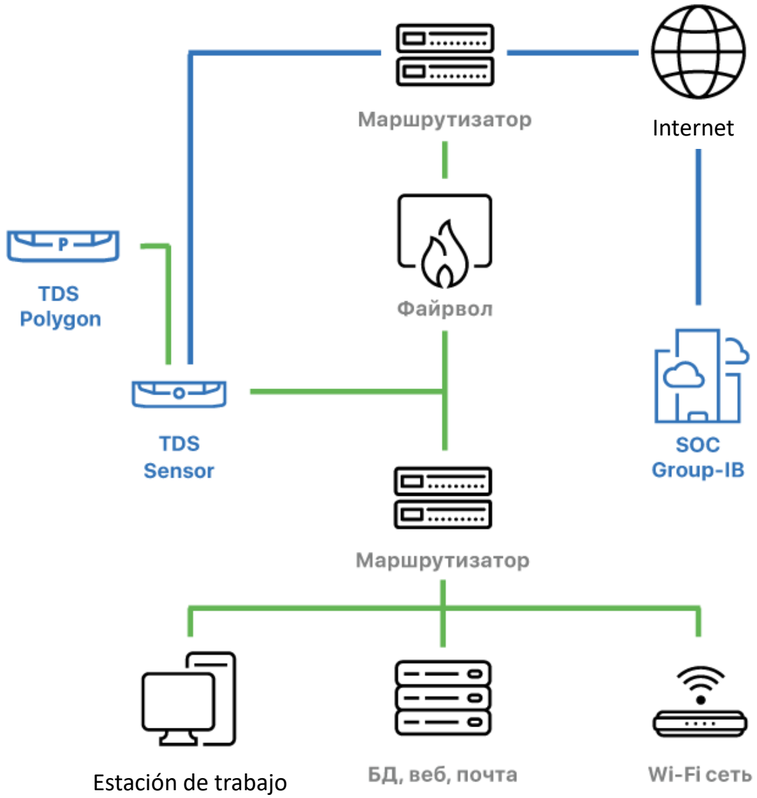
SENSOR DE ANÁLISIS DE TRÁFICO

Identifica los nodos infectados estableciendo su interacción con los centros de comando en función de los signos de actividad maliciosa, desarrollados sobre la base de datos de fuentes únicas.

Detecta anomalías de red generadas por programas maliciosos utilizando "algoritmos de aprendizaje automático".

Se integra con el sistema de análisis de comportamiento TDS Polygon ™ para detectar el código malicioso previamente desconocido.

Envía información sobre incidentes detectados en SOC Group-IB a través de un canal seguro o a cualquier sistema corporativo interno de contabilidad para eventos de IS.



SOC GROUP-IB

- La información sobre incidentes recibidos del sensor se clasifica y correlaciona en el Centro de datos.
- Los eventos son analizados por expertos calificados de Group-IB de forma manual.
- Los expertos de SOC notificarán a sus especialistas sobre amenazas críticas por teléfono y correo electrónico, y todos los resultados del análisis estarán disponibles en una conveniente interfaz web.

Los especialistas experimentados de Group-IB toman la responsabilidad de identificar incidentes críticos, permitiendo que su servicio IB se concentre en la respuesta.

Secure Bank

Sistema de alerta temprana para sistemas de pago

Detección proactiva de fraude bancario en todos los dispositivos y plataformas del clientes en tiempo real.

Nuestra solución:

- Evita el robo Mediante la detección temprana de fraude.
- Reduce los costos de procesamiento de alarmas falsas y llamadas a clientes.
- Aumenta la seguridad y el atractivo de sus sistemas bancarios en línea y móviles.
- Refuerza la confianza en el banco, brindando la oportunidad de advertir a los clientes sobre infecciones y ataques.

Secure Bank está incluido en el registro de software nacional

Secure Bank protege al "Sberbank en línea"

GROUP-IB

- Identifica los pagos fraudulentos y la preparación para su realización
- Detecta nuevos ataques y esquemas de fraude
- Actualización diaria de las reglas y firmas
- Soporte analítico y asesoramiento
- Módulo de JavaScript Para proteger el banco de Interne
- Mobile SDK para Android y iOS
- No requiere instalación. En el dispositivo del cliente

Cómo funciona Secure Bank

Secure Bank se carga junto con las páginas web del banco o la aplicación del banco móvil y le permite notificar al cliente de manera oportuna acerca de la infección o compromisos de su dispositivo.

El sistema identifica la inyección web maliciosa, ingeniería social, phishing, botnets, captura de cuentas, redes de conversión ilegal de dinero en efectivo y otros tipos de fraude bancario..

Tecnología Antifrood de Secure Bank

- Huella digital del dispositivo
- Perfil de usuario global
- Desarrollador de reglas avanzadas
- Análisis del comportamiento
- Detección sin agente de programas maliciosos
- Análisis de canales cruzados
- Datos del Group-IB Inteligencia de amenazas

Secure Bank usa medios ampliados para detectar programas maliciosos y su análisis de comportamiento para detectar fraudes antes de su origen

AF

Los sistemas clásicos de prevención de fraudes analizan las transacciones, pero ellos no detectan si los dispositivos de los clientes están infectados con programas maliciosos, si pasa algo sospechoso en ellos antes de la realización de la transacción

1. Intento de realización de acciones de fraude
(lanzamiento de programas maliciosos, ingeniería social, acceso remoto)

2. Realización de pago fraudulento

3. Retiro de dinero

El fraude puede durar desde algunos segundos hasta varios meses

Integración lista con la infraestructura del banco

BSS · R•Style Softlab · Intellinx Insider Threat Intelligence · FRAUDWALL · RSA · SAS · Radar · ArcSight An HP Company · POSITIVE TECHNOLOGIES

Identificación de amenazas que son invisibles a los sistemas antifraude tradicionales

Fraude de pago

- *Fraude de crédito*
- *Fraude con operaciones CNP*
- *Inyecciones malignas en la web*

Secure Bank ayuda a proteger los pagos electrónicos y los datos de las tarjetas de crédito de los clientes.

Robo de datos personales

- *Captura de cuenta*
- *Fraude de apertura de cuenta*
- *Acciones bots*

El sistema de análisis de comportamiento y la tecnología digital de "huellas dactilares" del dispositivo le permiten rastrear el uso de credenciales robadas.

Ingeniería social

- *Envíos fraudulentos*
- *Ataques dirigidos*
- *Phishing*

***La creación de un único perfil de cliente y el uso de los datos de Group-IB Inteligencia de amenazas previenen la fuga de datos y el fraude en la red*.**

Lavado de dinero

- *Redes de retiros ilegales*
- *Sistemas de evasión de impuestos*

El análisis de las interacciones entre cuentas y otras estructuras bancarias ayuda a identificar transacciones sospechosas

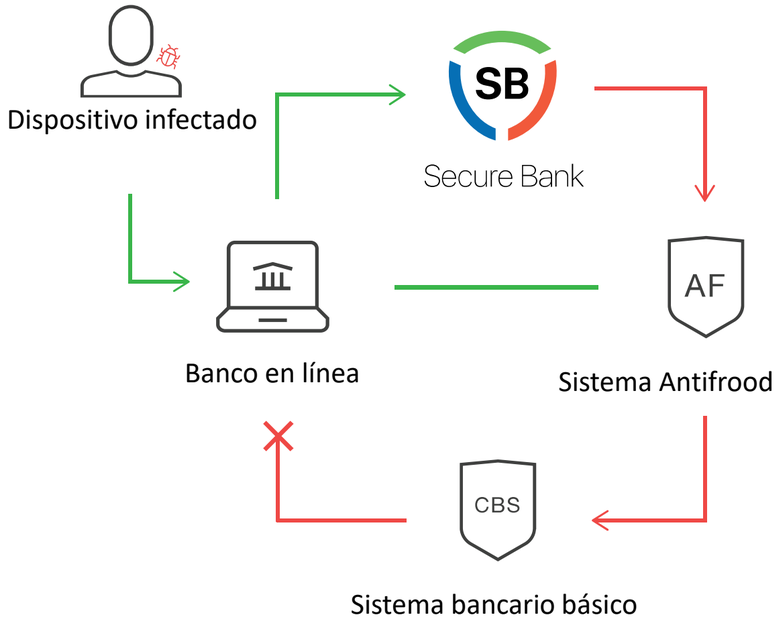
Programas maliciosos

- *Troyanos*
- *Farming*
- *Redes bot*
- ***Los algoritmos patentados de Secure Bank detectan troyanos bancarios sin instalar programas adicionales en el lado del cliente.***

Ataques entre canales y entre clientes

- *E-commerce*
- *Dispositivos móviles*
- *Interfaz web*

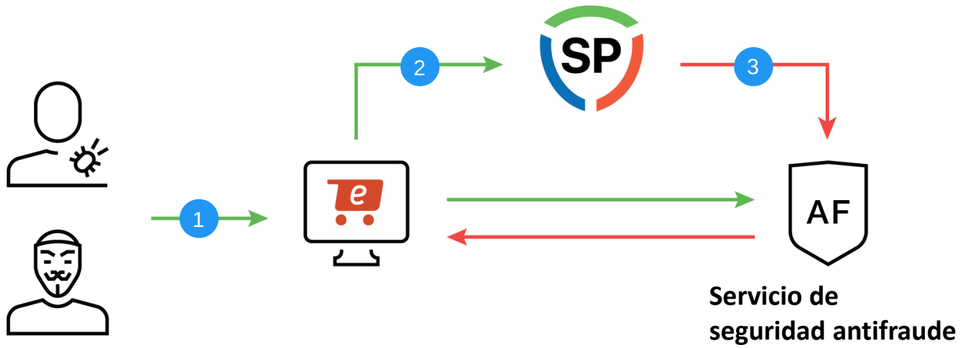
Secure Bank protege al cliente en todas las plataformas móviles y web, incluidas las tiendas en línea y los portales corporativos.



Portal seguro

Detección temprana de fraude por parte de los usuarios: el vínculo más débil en la seguridad de los portales de Internet

Incluido en el registro de software nacional



1. El módulo de JavaScript en la página del portal define una "huella digital" única del dispositivo del cliente y recopila indicadores de actividad fraudulenta
2. Los datos impersonales se transmiten a través de un canal seguro en SP, donde se procesa utilizando los datos del sistema Inteligencia de amenazas
3. El cliente recibe una notificación de fraude en tiempo real, API permite automatizar la respuesta a incidentes

La solución previene :

- Acceso de terceros a portales corporativos cerrados para fraude con puntos de bonificación
- Selección de contraseñas, envolvimiento de votos, colocación de evaluaciones falsas
- Uso compartido de suscripción pagada
- Interceptación de compradores mostrando anuncios de competidores en las páginas del portal

GROUP-IB

- Evita el robo de datos personales e información sobre tarjetas bancarias
- Identifica las compras de tarjetas robadas
- Evita el uso de bots
- No requiere inversión en la infraestructura de TI del portal
- API para integración con sistemas antifraude , SIEM, Firewall, EPS
- Soporte analítico y asesoramiento

Auditoría de seguridad de la información

Trabajamos con los principales bancos y nuevas empresas potenciales, gigantes energéticos y pequeñas oficinas de abogados, entendemos las debilidades de las infraestructuras de TI de cualquier escala y propósito.

- Sistemas RBS y aplicaciones de banca móvil
- Prevención de ataques DoS / DDoS, realizando pruebas de carga
- Corrección de la conmutación de redes de señalización de operadores de telecomunicaciones
- Recursos web, incluidos portales corporativos, estatales, sitios de comercio electrónico
- Pruebas socionotécnicas (ingeniería social)
- Escaneo de vulnerabilidad de infraestructuras de red
- Software, incluido iOS, Android, Windows Phone
- Investigación de seguridad POS, mPOS-terminales
- Sistemas para la protección de secretos comerciales y datos personales
- Software para sistemas de control de procesos y sistemas SCADA

Auditoría de seguridad de la información del Grupo IB:

- Analizamos vulnerabilidades por más de 10 años
- Nos sumergimos profundamente en la lógica interna de sus sistemas.
- vemos los riesgos que escapan del campo de visión de los demás
- Cada informe contiene "un breve resumen para los responsables de la toma de decisiones", y una descripción detallada "y recomendaciones específicas para los especialistas".

Evaluación de compromiso

Identifica los rastros de compromiso y signos de preparación de un ataque de piratas informáticos.

La evaluación de compromiso identificará rastros de preparación para el ataque de piratas informáticos, signos de compromiso de datos, ayuda a evaluar la escala del daño y descubrir qué sistemas fueron atacados y cómo sucedió exactamente.

En base a los resultados de la evaluación de compromiso:

1. **Informe sobre compromisos**
   Descripción de la cronología de la infraestructura de compromiso, análisis detallado de las acciones de los intrusos
2. **Informe sobre el trabajo realizado**
   Descripción detallada de la composición del trabajo y los resultados en cada etapa de la evaluación de compromiso
3. **Recomendaciones**
   Recomendaciones para actualizar la infraestructura para prevenir futuros ataques
4. **Informe para la administración**
   Un breve informe que describe los principales resultados de la verificación de la infraestructura

Los expertos de Group-IB identificarán las amenazas ocultas antes de que usted sufra un daño real

En el marco de la evaluación de compromiso, los especialistas del Grupo IB instalarán el complejo de software y hardware TDS, y los expertos con cientos de investigaciones analizarán la infraestructura e identificarán signos de compromiso.

.

Los expertos en informática criminalística verificarán los elementos claves de la infraestructura con el tema de compromiso

- Utilizan herramientas forenses especializadas de diseño propio e información única sobre Inteligencia de amenazas.
- Comprueba los nodos clave de la infraestructura: controlador de dominio, procesamiento, pasarelas de pago, etc.
- Restaura la cronología de la infraestructura comprometida para evitar la recurrencia de incidentes

El complejo TDS ayudará a identificar signos anteriores inadvertidos del ataque cibernético dirigido

- El sensor TDS detecta anomalías en la red, infecciones y comportamiento inusual de los dispositivos
- TDS Polygon lanza objetos potencialmente peligrosos en un entorno aislado, analiza el comportamiento del objeto y determina el grado de peligro
- Todos los eventos identificados son analizados por especialistas en modo 24/7

Usted no puede ver las amenazas ocultas durante meses

Preparación para el ataque dirigido

Los piratas informáticos despliegan la infraestructura para atacar durante varios meses, desapercibido para usted

Fusiones y Adquisiciones

La integración con otro negocio conlleva a riesgos ocultos en la nueva infraestructura: marcadores, puertas traseras, CVE

Competidores desleales

Al obtener acceso a secretos comerciales, los competidores proporcionan su propia ventaja en el mercado

Insiders o empleados despedidos

Al saber cómo funciona la infraestructura de la empresa, silenciosamente "fusionan" los datos y permanecen desapercibidos durante mucho tiempo

Red Teaming

Imitación regular de ataques dirigidos para fortalecer sus servicios de seguridad. Ejercicios a escala completa que involucran a su servicio de seguridad, que proporcionará respuestas a las siguientes preguntas:

- ¿ Están listos sus sistemas para prevenir, detectar y reaccionar eficazmente a los incidentes?
- ¿Cómo actúan los agentes de seguridad? ¿Durante un ataque dirigido?
- ¿Qué se debe cambiar exactamente en sus enfoques de seguridad para aumentar la capacidad de la empresa para resistir los ataques?

Como resultado de la imitación regular de ataques, Red Teaming ayuda a aumentar la preparación para ataques dirigidos, identificar y eliminar nuevas vulnerabilidades, capacitar a su equipo y mejorar procesos para contrarrestar amenazas reales.

En base a los resultados de Red Teaming:

- Breves informes para la administración
- Informes detallados sobre los resultados y consejos de expertos para mejorar su sistema de seguridad
- Alertas de emergencia, en el caso de Detección de vulnerabilidades críticas

Red Teaming Methodology:

Coordinación de objetivos, elección de herramientas → Durante varios meses: imitación regular de ataques dirigidos, en donde solo el jefe del Servicio de Seguridad es advertido → Monitoreo constante de los cambios en su infraestructura que abren una nueva superficie para el ataque

Red Teaming no está limitado en el tiempo . Este enfoque ilimitado lleva a Red Teaming lo más cerca posible del modelo de comportamiento de un atacante real que puede prepararse para un ataque durante meses, probando diferentes herramientas y vectores de ataque.

El término Red Teaming vino de asuntos militares: durante los ejercicios el equipo rojo ataca, el "azul" se defiende.

Protección de marcas

Servicio tecnológico para identificar y eliminar amenazas dirigidas contra marcas en Internet.

Evitamos las pérdidas de dinero y reputación de las empresas frente a amenazas reales en línea:

- Uso no autorizado de la marca y fraude en Internet
- Propagación de la falsificación y el incumplimiento de la política de socios
- Ataques de información y críticas negativas

Violaciones de tecnologías de búsqueda avanzada:

Aprendizaje automático
El sistema mismo califica violaciones basadas en experiencias previas

Big data
La gran tecnología de análisis de datos identifica automáticamente los enlaces entre sitios y entre grupos en las redes sociales

Intelligence driven
Technologies Group-IB, utilizado en la investigación del cibercrimen, permite establecer contacto directo con infractores

3 millones de recursos
rastreado automático en modo 24/7

10 mil
las violaciones son eliminadas todos los días

85% de violaciones
se eliminan en el pre-juicio

Bloqueo rápido de sitios peligrosos

Capacidad de reaccionar fuera del Runet

Monitoreo las 24 horas

Colección de evidencia digital

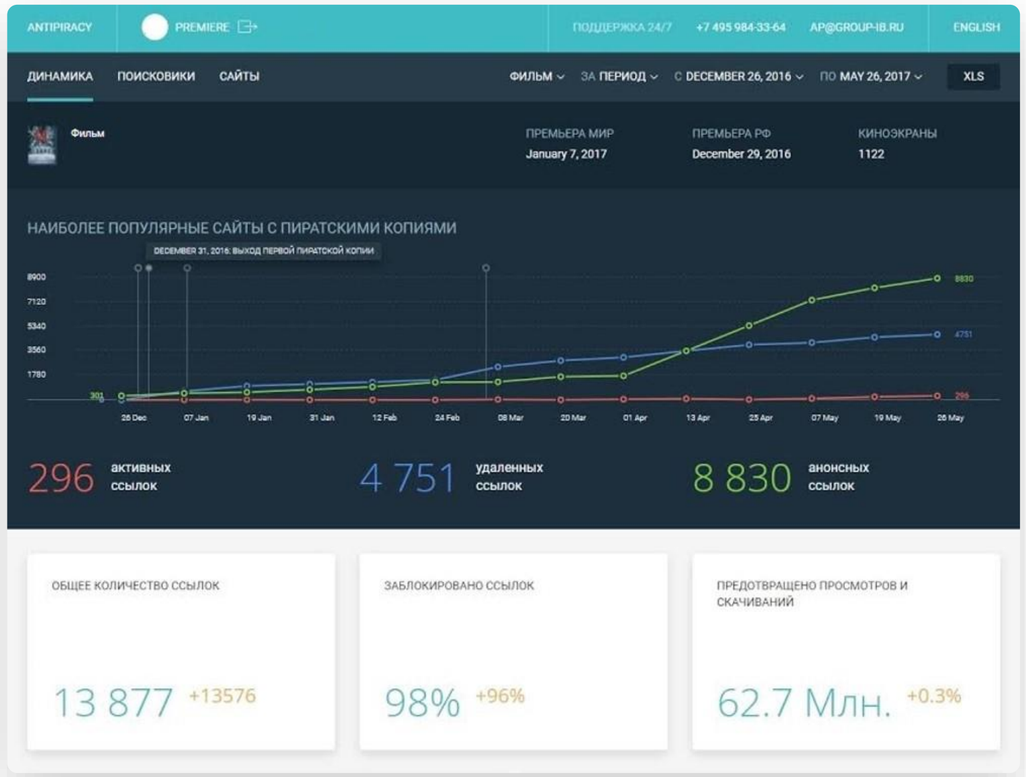
Identificación de enlaces entre sitios fraudulentos

Previención de "recaídas"

Anti piratería

El líder del mercado de protección inteligente de contenido digital

- Monitoreo de más de 120 000 recursos, incluidos vk.ru, veterok.tv, kinostock.tv
- Casos exitosos de bloqueo judicial de sitios piratas
- Bloqueo en línea de contenido en grandes sitios piratas
- Redirige a los usuarios a sus recursos oficiales



En 30 minutos
encuentra contenido pirata, incluso sometido a cambios significativos

24 horas
Suprimimos la distribución de contenidos a los mayores sitios piratas de runet

7 días
bloquea hasta el 99% de los enlaces de su contenido y ofrece soluciones para sitios intratables

- Correcto diseño de bloqueo
- Alto retorno de las notificaciones
- Interfaz intuitiva entendible
- Monitoreo las 24 horas
- Amplia gama de medidas previas al juicio
- Eliminación del contenido pirata con un botón

Centro de respuestas CERT-GIB

CERT-GIB (Equipo de respuesta de emergencia informática) — centro de respuesta las 24 horas a incidentes de seguridad de la información

- Controlamos la aparición de recursos phishing, la propagación de software malicioso y el comercio de productos falsificados
- Proporcionamos soporte legal completo en todas las etapas de la respuesta e investigación
- Bloqueamos rápidamente sitios web peligrosos en .RU, .РФ, e incluso más de 1000 zonas de dominio
- Trabajamos en todo el mundo: a través de una red de socios, contacto con proveedores de hosting y registradores de nombres de dominio

Rosteh, una de las corporaciones estatales más grandes de Rusia, eligió Group-IB como socio para crear su propio CERT RT-Inform

Organización competente del Centro de coordinación del dominio nacional de Internet y del Fondo de desarrollo de Internet

Miembro acreditado de comunidades internacionales FIRST y Trusted Introducer

Socio de IMPACT - Asociación internacional para contrarrestar las amenazas cibernéticas

Autorizado por la Universidad de Carnegie, oficialmente utiliza la marca CERT

Laboratorio de informática criminalística y departamento de investigación

El Laboratorio de Informática criminalística y Análisis de Código Malicioso más grande en Europa del Este

El equipo más moderno y análisis viral avanzado

Los mejores desarrollos mundiales, que permiten eludir la tecnología de ocultar rastros.

Interacción con agencias policiales

Incluida la participación oficial en actividades de búsqueda operativa

Buscar datos en cualquier medio

Encontraremos los datos, incluso si fueron eliminados, ocultos o encriptados

Equipo de respuesta móvil

Recopilación e investigación de pruebas digitales "sobre el terreno, recomendaciones" para eliminar las consecuencias

---

80% de los delitos resonantes de alta tecnología en Rusia se investigan con la participación de nuestros especialistas

Encontraremos un enfoque individual para cada uno

Un equipo de especialistas: desde "E-Discovery y Forensic " hasta la auditoría financiera y el derecho corporativo

Tenemos experiencia en recuperar los activos retirados

3.3 mil millones de rublos fueron devueltos a la compañía lesionada como resultado de una de las investigaciones

Comprendemos la economía del cibercrimen

Restauramos el flujo de dinero con la ayuda exclusiva de los datos de inteligencia de Inteligencia de amenazas

Asesoramos a abogados, investigadores y fiscales

Las consultas son posibles en todas las etapas de la investigación

- Examinación técnica computarizada
- Amplia experiencia en la presentación de pruebas digitales en los tribunales
- Recolección de evidencias digitales
- Investigación de programas maliciosos
- Outsourcing y examinación independiente
- Investigación forense

PRE-IR ASSESSMENT

Preparación para una respuesta efectiva a incidentes de seguridad de la información.

Pre-IR Assessment ayudará a verificar la preparación de sus sistemas, equipos y procesos para responder y elaborar un plan claro en caso de un incidente.

Problemas típicos

- Se pierde una gran cantidad de datos o su registro no se realiza correctamente
- El incidente causa pánico y acciones descontroladas
- Los procesos de respuesta no son uniformes, los roles no están distribuidos

Resultados Pre-IR Assessment

- Recomendaciones para configurar sistemas para una respuesta efectiva a un incidente
- Confianza y un plan de acción claro y bien definido
- Comunicaciones bien establecidas entre departamentos

Evaluación completa de los principales componentes

1 Tecnología

Verificación de la red y la infraestructura del sistema: la posibilidad de recopilación completa y correcta de evidencia digital, la capacidad de identificar indicadores de compromiso, la capacidad de detener rápidamente el incidente y gestionar la red durante la respuesta.

El resultado es el desarrollo de procesos en sistemas reales: ejecución de scripts, búsqueda y recopilación de datos necesarios para varios tipos de incidentes.

2 Gente

Verificación de la competencia de los empleados de servicios de TI y seguridad de la información.

El resultado es una capacitación de dos días sobre la respuesta a incidentes de expertos del Grupo IB, un equipo seguro y bien capacitado.

3 Regulaciones

Verificación de integridad, relevancia y conveniencia práctica de regulaciones y documentación.

El resultado son regulaciones y documentos que serán realmente útiles en caso de incidente.

4 Estructura

Verificación de la distribución de responsabilidades y la estructura organizacional del equipo.

El resultado es el trabajo coordinado y en equipo de los diversos departamentos durante la respuesta al incidente.

Cómo pasar Pre-IR Assessment

Preparación

- Recopilación de información
- Adaptación del programa para un cliente e industria específicos
- Aprobación de las reglas de inspección
- Términos acordados

El proceso

- Salida de los expertos del Grupo IB a la empresa cliente
- Solicitud de datos típicos para diferentes incidentes
- Análisis de integridad, disponibilidad y velocidad de adquisición de datos
- Realización de capacitación sobre respuesta a incidentes

- **Resultado**
- Recomendaciones para configurar sistemas para una respuesta efectiva
- Optimización de la estructura y los procesos
- Plan de respuesta
- Regulaciones preparadas
- Equipo entrenado

Hemos estado previniendo e investigando el cibercrimen desde 2003.

www.group-ib.ru
info@group-ib.ru
twitter.com/groupib
t.me/group_ib
group-ib.ru/blog
+7 495 984 33 64
facebook.com/group-ib
instagram.com/group_ib