EBRAX
ATM SECURITY LLC

Especialistas en seguridad

CIBERNÉTICA BANCARIA

EBRAX ATM SECURITY LLC
info@gigsrl.com

Nuestras soluciones en Seguridad Bancaria se utilizan en más de

40 Instituciones Financieras

las cuales acompañamos mediante nuestra experiencia para hacer que su negocio sea más Estable, duradero y Seguro.

Experiencia Servicios Profesionales

Algunos de nuestros clientes son de los más reconocidos en medios de banca y pagos

Contamos con más de 40 Clientes en la Región LATAM

Servicos Profesionales

EBRAX ATM SECURITY LLC
info@gigsrl.com

Servicios
PROFESIONALES ATM's

- **Hacking Ético** a todas las marcas versiones y modelos de hardware y software para ATM
- **"Tunning"** de aplicaciones para ATMs
- **Solución de** Anti-BlackBox
- **Diseño de soluciones** de monitorización y seguridad a medida para ATMs de cualquier Software XFS.
- **Auditoría de Servidor** de transacciones y protocolos NDC, DDC, ANDC.
- **Reversing y Forense** de todas las marcas de software y hardware de ATM

Servicios PROFESIONALES PoS

- **Hacking Ético** a todas las marcas de Hardware y desarrollos de software para equipos PoS
- **Asesoría y acompañamiento** en procesos de adquisición de Soluciones de seguridad
- **Desarrollo de soluciones** de monitorización y seguridad a medida para PoS
- **Auditoría de aplicaciones** PoketPoS o Mobile+PoS
- **Auditoría de servidor** de transacciones y Red

Servicios
PROFESIONALES BIGDATA

Resolución de problemas de Almacenamiento, procesamiento y estructuración de datos para la aplicación de soluciones avanzadas en el mercado entre ellas:

- **Desarrollo de reportes** basado en inserción de datos masivos.
- **Diseño de algoritmos** y procesamiento para la optimización de datos.
- **Aplicación de algoritmos** de Inteligencia Artificial para múltiples casos de uso.
- **Aplicación de patrones** de antifraude.
- **Determinación avanzada** de perfiles y sentimientos.

Nuestros Productos

EBRAX ATM SECURITY LLC
info@gigsrl.com

Producto
Browser Security Banca Online

Protege a tus clientes de ataques más complejos que no pueden ser protegidos sólo por la aplicación y controles de red

Anti-Phising protege a tus clientes de posibles engaños

Anti-Malware protege a tus clientes de ataques de malware infectando su escritorio

Endurecimiento de controles de navegador Mejora las configuraciones del navegador de tus clientes

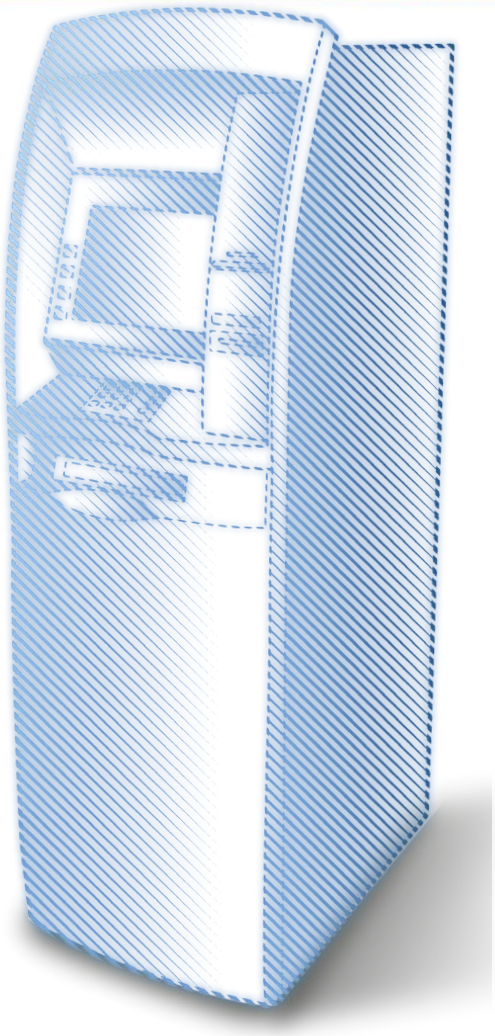
Detección de anomalías comprueba la Fé de vida del cliente y no que sea algún atacante o secuestro de sesión

XFS ANALYTICS

El tiempo máximo para la resolución de un caso individual no excede los

3 minutos, esto aumenta el tiempo de resolución del problema en un 99,95%

y evitará que la investigación llegue a días, semanas o incluso en los casos más difíciles a un mes.



Disminuya la necesidad de contar, en sus tareas diarias, con personal altamente especializado y dedicado para identificar y analizar los problemas en la red de cajeros automáticos que controla el proveedor de hardware y el reabastecimiento en efectivo.

Ahorre tiempo y recursos en el análisis de cualquier tipo de problema en la red de cajeros automáticos de cualquier marca.

Posea un análisis imparcial y veraz de la información recopilada en tiempo real.

Tenga una recopilación de información y un procesamiento completamente seguros.

Producto
SDK Security Android

Protege a tus clientes y a sus teléfonos android con las últimas protecciones a nivel de aplicación

- DETECCIÓN DEBBUGER
- DETECCIÓN ROOT
- DETECCIÓN EMULADOR
- DETECCIÓN OVERLAY
- DETECCIÓN REPACKING
- DETECCIÓN CODE INJECTION
- KEYLOGGERS & SCREEN READERS
- DETECCIÓN HOOKING
- LISTADO DE APLICACIONES INSTALADAS FUERA DE TIENDAS OFICIALES
- LISTADO DE APLICACIONES INSTALADAS DE TIENDAS OFICIALES
- DETECCIÓN DE SNIFFER
- DETECCIÓN DE PROXY
- DETECCIÓN SCREENSHOT
- OBTENCIÓN DE LISTADO DE APLICACIONES Y CLASIFICACIÓN DE AMENAZAS
- LISTADO DE CERTIFICADO INSTALADOS Y VÁLIDOS
- OBTENCION DE PROCESOS Y CLASIFICACIÓN DE AMENAZAS INSTALADAS Y EJECUTÁNDOSE

XFS ANALYTICS

La solución de monitorización de ATM & PoS más avanzada del mercado

L = Ataque lógico
P = Ataque físico
ON = Requiere presencia constante
OFF= No Requiere presencia constante

TIPOS DE ATAQUES
QUE DETECTA **XFS** ANALYTICS

Ataques Presenciales

(P-OFF) Ram raid
(P-OFF) Smash and grab
(P/L-ON) Card trapping
(P/L-ON) Skimming
(P/L-ON) Shimming
(P-ON) TRF I / II
(P-ON) Cash trapping I / I

Ataques Lógicos

(L-OFF) Malware
(L-OFF) Unauthorized management applications and services
(L-ON/OFF) PAC=MITM
(L-OFF) Black box
(L-ON) Malicious dispense orders
(L-ON) Malware distribution
(L-ON) Active Man-in-the-middle (A-MITM)
(L-ON) Passive Man-in-the-middle (P-MITM)
(L-OFF) Host spoofing

Algunos ataques físicos los detectamos conectándonos a soluciones perimetrales.

CARACTERÍSTICAS
XFS ANALYTICS

- Detección de errores de reposición de efectivo.
- Analizar casos de faltantes de efectivo en tiempo real de múltiples ATM al mismo tiempo.
- Extracción de resultados en PDF o por correo.
- Almacenamiento de información en un entorno seguro y confiable.
- Accesos y control de roles para todos los procesos de análisis de información.
- Interfaz interactiva con gestión de locaciones de ATMs/PoS.
- Gestión de Roles y permisos para acceso a información.
- Gestión de Logs y eventos de PoS

REQUISITOS de XFS ANALYTICS

- **Sistema Operativo**
  Windows XP o 7

- **Hardware**
  Todos los modelos de NCR Diebold-Nixdorf (Diebold y Wincor Nixdorf) WRG, Fujitsu, Nautilus y otros.

- **XFS ANALYTICS**
  Kal, Agilis, APTRA, Procash / Probase Dynasty, JXFS, Phoenix, XFS y muchos otros.

OPERACIONES DETECTADAS

- Errores en las Tarjeta
- Errores Faltantes
- Errores en las Transacciones
- Errores en la impresión
- Errores en los depósitos
- Posibles Errores en el Modo Mantenimiento

ATX
CORE SECURITY

Introducción

ATX Core Security

ATX Core Security es un software de seguridad y protección contra los ataques informáticos avanzados, dirigidos a Cajeros Automáticos (ATMs).

La primera capa de protección física permite conectarte y reportar eventos de soluciones como anti-skimming y cerraduras electrónicas y solución anti-blackbox para determinar acciones preventivas frente ataques.

La segunda capa permite controlar aspectos del control de BIOS para proteger el acceso o carga de software malicioso desde antes del arranque del sistema operativo y además proteger el propio disco.

La tercera capa permite ejecutar controles de sistema operativo enfocados en la protección y integridad de las operaciones del software

Además, el software puede configurarse para operar con otros módulos de correlación y detección de operaciones en el cajero automático ATM.