INFORME TECNICO DE SEGURIDAD CIBERNÉTICA DE OPERACIONES E INTELIGENCIA

Metrobank S.A.

Diciembre, 2018

Tel: +1 609-651-4246
Tel: +507-836-5355

Info@glesec.com
www.glesec.com

CONFIDENCIAL

Tabla de contenido

USA | PANAMA | ARGENTINA | MEXICO | COLOMBIA | PERU | CHILE | ECUADOR
Tel: +1 (609)-651-4246 / +(507)-836-5355

Sobre este informe

Este informe es un complemento del Informe ejecutivo mensual de inteligencia y operaciones. El propósito de este documento es proporcionar información a nivel técnico y táctico, detalles y recomendaciones en la medida en que puedan resumirse. GLESEC procesa una gran cantidad de datos y no todos pueden presentarse en un formato de informe detallado. Para obtener más información, puede consultar los paneles de la GMP o, si es necesario, comuníquese con nosotros en los Centros de operaciones de GLESEC (GOC).

Confidencialidad

GLESEC considera la confidencialidad de la información de los clientes como un secreto comercial. La información bajo este contexto se clasifica como:

- Nombre e información de contacto del cliente
- Arquitectura del sistema, configuración, métodos de acceso y control de acceso
- Contenido de seguridad

Todo lo mencionado arriba es resguardado de manera segura de la misma forma como GLESEC resguarda su propia información confidencial.

Servicio Externo Administrado de Vulnerabilidad (MSS-VME)

El Servicio Externo Administrado de Vulnerabilidades (MSS-VME) permite a las organizaciones minimizar el riesgo de vulnerabilidades en el perimetro (o desde el Internet) descubriendo rápidamente las debilidades, midiendo el riesgo potencial y la exposición, informando, proporcionando la información de remediación necesaria para mitigar esos riesgos de manera continua y facilitando la presentación de informes y el cumplimiento Con normativa y mejores prácticas.

Definiendo sistemas críticos

Definimos "sistemas críticos" como los hosts, servidores y aplicaciones que son "las más importantes" para las operación del negocio de nuestros clientes-miembros. Esta calificación de "más importante" queda a criterio de la organización miembro-cliente.

*Esta lista de sistemas críticos fueron proporcionados por el cliente a través del formulario **"TIP^{tm} Information Gathering Critical Assets"**, cualquier cambio que se deba realizar por favor notificarnos.*

Nombre del Host, servidor o aplicación	Tipo de sistema	Dirección IP
Web Govimar	Windows	190.34.183.131
Web Metrobank	Windows	190.34.183.152
AppServer	Windows	190.34.183.139
MailMarshal	Windows	190.34.183.148
Exchange	Windows	190.34.183.149
Ebanking IBM	Windows	190.34.183.154
Ebanking	Windows	190.34.183.153

*En la sección de **Correlación entre los servicios MSS-APS y el MSS-VME** pag.16, obtendrá información respecto a los ataques que reciben estos sistemas críticos e igualmente las vulnerabilidades presentes.*

Para este período y según el rango de direcciones proporcionadas por Metrobank S.A., el número total de hosts analizados es de 16, de los cuales en 11 de ellos se encontró al menos una vulnerabilidad. Estas vulnerabilidades se dividen en las siguientes severidades como se muestra en la siguiente tabla. Además, puede observar la puntuación de valor de riesgo de su organización según nuestras métricas, que ha aumentado en comparación con el mes pasado.

Total IP's Scanned	IP's Vulnerable
15	11

Risk Distribution				
Critical	High	Medium	Low	Total
2	6	34	22	64

According to the metrics:
RV= 0.294479167

The following values are to clarify RV:
RV=1 Points to every IP address in the infrastructure that are susceptible to attacks
RV=0 Points to no IP address in the infrastructure aret susceptible to attacks
RV=0.1 Point to 1/10 IP address in the infrastructure that are susceptible to attacks

Todas las vulnerabilidades encontradas en su organización pertenecen a las siguientes categorías:

Category	Critical	High	Medium	Low	Total
General	0	0	28	8	36
Misc.	0	1	5	10	16
Service detection	0	5	0	3	8
Windows	2	0	1	0	3
Web Servers	0	0	0	1	1

- General (56%).
- Misc (25%).
- Services Detection (12.5%).
- Windows (5%).
- Web Servers (1.5%).

Para detalles adicionales sobre estas vulnerabilidades se encontraron en Metrobank S.A, favor referirse a la sección de severidad del MSS-VM en la página 9.

Metrobank S.A continúa presentando vulnerabilidades críticas (3%), altas (9%), medias (53%) y bajas (34%). Para este mes, *en todos los escaneos del servicio MSS-VME realizados en cada semana se pudieron observar que se han mantenido la mismos cantidad de hosts vulnerables y la distribución de vulnerabilidades en comparación al mes anterior*.

Principales categorías que tienen más vulnerabilidades:

- General (56%) presenta en su mayoría vulnerabilidades de tipo SSL, como las suites de cifrado de fuerza media y el certificado SSL no confiable. Estos representan un nivel medio de severidad.

- Misc. (25%) presenta las principales vulnerabilidades de tipo: SSH Server CBC Mode Ciphers Habilitado, Logjam representa un bajo nivel de severidad y SSH soporta algoritmos débiles, SSL / TLS DROWN.

- Service Detection (12.5%) presenta principalmente el tipo de vulnerabilidad: la detección de los protocolos SSL versión 2 y 3 representa un alto nivel de severidad; y también presenta SSL Anonymous Cipher Suites Supported, que tiene un bajo nivel de severidad.

- Windows (5%) su principal vulnerabilidad es MS15-034: Una vulnerabilidad en HTTP.sys podría permitir la ejecución remota de código (3042553) (verificación sin credenciales) representa un nivel de riesgo crítico y Desglose de información en el Client Access Server de Microsoft Exchange de severidad media.

- Web Servers (1.5%) presenta encabezado HTTP puede revelar dirección IP interna esta vulnerabilidad representa un nivel de riesgo bajo.

De todos los tipos de vulnerabilidades mencionados anteriormente, los que se presentan con frecuencia son los paquetes de cifrado SSL de potencia media compatibles (15%) y el certificado SSL no se puede confiar (8%).

Entre las vulnerabilidades que presentan un nivel de gravedad crítica y alta tenemos:

- La vulnerabilidad de HTTP.sys permite la ejecución remota de código (3042553) (verificación sin credenciales). Existe una actualización de seguridad que se considera fundamental para todas las ediciones compatibles de Windows 7, Windows Server 2008 R2, Windows 8, Windows Server 2012, Windows 8.1 y Windows Server 2012 R2.
  Hosts afectados 190.34.183.131,190.34.183.139.

- La vulnerabilidad de detección del protocolo SSL versiones 2 y 3 se considera de alta severidad y se presenta en los hosts 190.34.183.142, 190.34.183.149, 190.34.183.154, 190.34.183.139 y 190.34.183.152.

Los 4 puertos considerados más vulnerables para este período fueron 443 (HTTPS) 22 (SSH), 25 (SMPT) y 80 (HTTP). Esto se debe al hecho de que se encontraron muchas vulnerabilidades relacionadas con ellas y que la mayoría se clasifica en un nivel de gravedad medio, excepto en el puerto 80 que tiene un nivel de gravedad crítico.

A continuación, se muestran los hosts más vulnerables para estos puertos:

- 443 (HTTPS) La mayoría de los hosts son vulnerables por este puerto, entre ellos tenemos: 190.34.183.139, 190.34.183.142, 190.34.183.152, 190.34.183.154, 190.34.183.149, 190.34.183.132, 190.34.183.131 190.34.183.91 y 190.34.183.90.

- 22 (SSH) Las vulnerabilidades presentadas por este puerto son: Algoritmos débiles SSH admitidos, Cifrados en modo CBC del servidor SSH habilitados y Algoritmos MAC débiles SSH habilitados y versión desactualizada de libssh. Los hosts afectados son 190.34.183.81 y 190.34.183.142.

- 80 (HTTP) Los hosts que presentan vulnerabilidad por este puerto son 190.34.183.131 y 190.34.183.139, es una vulnerabilidad crítica como se mencionó anteriormente "Vulnerabilidad de HTTP.sys Permitir la ejecución remota de código (3042553).

El puerto que aparece con mayor frecuencia como vulnerable es 443.

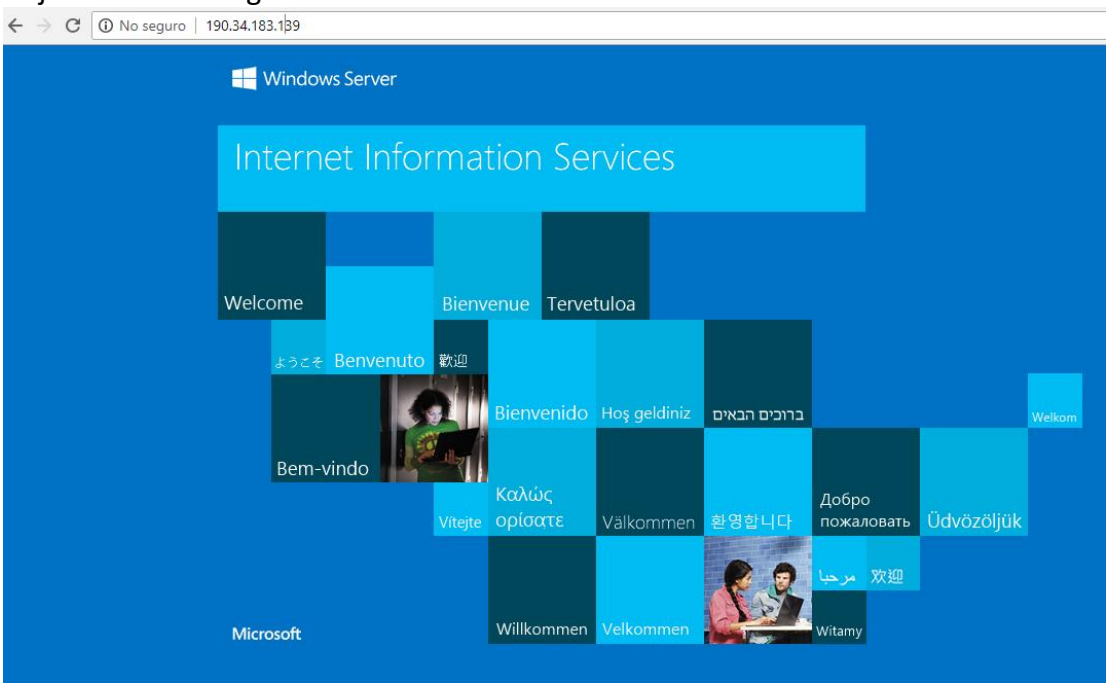
Los hosts más vulnerables son: 190.34.183.142, 190.34.183.139, 190.34.183.152, 190.34.183.149; La mayoría son de severidad media y baja.

Descripción por Host

El host remoto http://190.34.183.139/ Se ve afectada la acción de Fingerprinting. Esta vulnerabilidad es conocida como OS Fingerprinting es una técnica que consiste en analizar las huellas dejadas por un sistema operativo en sus conexiones de red. Se basa en los tiempos de respuesta a los diferentes paquetes, para establecer una conexión en el protocolo TCP / IP, que es utilizado por los diferentes sistemas operativos. Recomendamos aplicar más seguridad a sus servidores.

También en este host hemos detectado SSL versión 2 y versión 3. Este protocolo es considerado inseguro según estándares modernos, la práctica recomendada es implementar el protocolo TLS versión 1.1 o superior. El uso del protocolo SSL v2 y 3 expone el equipo a ataques como POODLE y DROWN.

Adjuntamos la imagen del host vulnerable.



El host remoto 190.34.183.131 (https://www.govimar.com.pa/) es afectado por la vulnerabilidad HTTP.sys podría permitir la ejecución remota de código (3042553), que afecta a los sistemas Windows (puertos 80/443); Recomendamos aplicar todas las actualizaciones de seguridad sugeridas por Windows, especialmente MS15-034 (KB 3042553), ya que todas resuelven las vulnerabilidades encontradas en este tipo de sistema. El mes anterior se presentó esta vulnerabilidad.

Vulnerabilidades por severidad

La siguiente sección describirá en detalle cada vulnerabilidad encontrada de acuerdo con su severidad.

Vulnerabilidades de severidad critica

MS15-034: Vulnerability in HTTP.sys Could Allow Remote Code Execution

Descripción
La versión de Windows que se ejecuta en el host remoto se ve afectada por una condición de desbordamiento de entero en la pila de protocolo HTTP (HTTP.sys) debido al análisis incorrecto de las solicitudes HTTP elaboradas.
Solución
Microsoft ha lanzado un conjunto de parches para Windows 7, 2008 R2, 8, 8.1, 2012 y 2012 R2.

Sistemas Afectados

80 / tcp / possible_wls	190.34.183.131, 190.34.183.139
443 / tcp / possible_wls	190.34.183.131, 190.34.183.139

Vulnerabilidades de severidad Alta

SSL Version 2 and 3 Protocol Detection

Descripción
El servicio remoto acepta conexiones cifradas utilizando SSL 2.0 y / o SSL 3.0. Estas versiones de SSL se ven afectadas por varios defectos criptográficos.

Solución
Consulte la documentación de la aplicación para deshabilitar SSL 2.0 y 3.0.
Utilice TLS 1.2 (con conjuntos de cifrado aprobados) o superior en su lugar.

Sistemas afectados
443 / tcp / possible_wls 190.34.183.139, 190.34.183.149, 190.34.183.154, 190.34.183.152.

Vulnerabilidades de severidad media

SSL Medium Strength Cipher Suites Supported

Descripción
El host remoto admite el uso de cifrados SSL que ofrecen cifrado de intensidad media. GLESEC considera la fuerza media como cualquier cifrado que usa longitudes de clave de al menos 64 bits y menos de 112 bits, o bien que utiliza el conjunto de cifrado 3DES.

Solución
Reconfigure la aplicación afectada si es posible para evitar el uso de cifrados de resistencia media

Sistemas Afectados
9443,8089 / tcp / possible_wls 190.34.183.139
443 / tcp / possible_wls 190.34.183.132, 190.34.183.139, 190.34.183.149, 190.34.183.152, 190.34.183.154, 190.34.183.90, 190.34.183.91

SSL Certificate Cannot Be Trusted

Descripción
El certificado X.509 del servidor no es confiable

Solución
Genere certificados de confianza.

Sistemas Afectados

25 / tcp / smtp 190.34.183.148
443 / tcp / possible_wls 190.34.183.90, 190.34.183.91, 190.34.183.132

SSL Certificate Signed Using Weak Hashing Algorithm

Descripción
El servicio remoto utiliza una cadena de certificados SSL que se ha firmado con un algoritmo de hashing criptográficamente débil (por ejemplo, MD2, MD4, MD5 o SHA1). Se sabe que estos algoritmos de firma son vulnerables a los ataques de colisión. Un atacante puede explotar esto para generar otro certificado con la misma firma digital, permitiendo que un atacante se haga pasar por el servicio afectado.

Tenga en cuenta que este complemento informa de todas las cadenas de certificados SSL firmadas con SHA-1 caducaron el 1 de enero del 2017.

Sistemas Afectados
443 / tcp / possible_wls 190.34.183.132, 190.34.183.90, 190.34.183.91

SSLv3 Padding Oracle On Downgraded Legacy Encryption Vulnerability(POODLE)

Descripción
El host remoto se ve afectado por una vulnerabilidad de divulgación de información de man-in-the-middle (MitM) conocida como POODLE. La vulnerabilidad se debe a la forma en que SSL 3.0 maneja los bytes de relleno al descifrar mensajes encriptados usando cifrados de bloque en el modo de encadenamiento de bloques de cifrado (CBC).

Solución
Deshabilitar SSLv3.

Sistemas Afectados
443 / tcp / possible_wls 190.34.183.142, 190.34.183.149

SSL/TLS EXPORT_RSA <= 512-bit Cipher Suites Supported (FREAK)

Descripción

El host remoto admite conjuntos de cifrado EXPORT_RSA con claves menores o iguales a 512 bits. Un atacante puede factorizar un módulo RSA de 512 bits en un corto período de tiempo.

Sistemas Afectados

- 190.34.183.154,190.34.183.152,190.34.183.139

Vulnerabilidades de severidad baja

SSL RC4 Cipher Suites Supported (Bar Mitzvah)

Descripción

El host remoto admite el uso de RC4 en una o más suites de cifrado.
El cifrado RC4 tiene fallas en su generación de un flujo de bytes pseudoaleatorios, por lo que se introduce una amplia variedad de pequeños sesgos en el flujo, lo que disminuye su aleatoriedad.

Solución

Reconfigure la aplicación afectada, si es posible, para evitar el uso de cifrados RC4. Considere el uso de TLS 1.2 con las suites AES-GCM sujetas a soporte de navegador y servidor web.

Sistemas Afectados

443 / tcp / possible_wls190.34.183.139,190.34.183.149,190.34.183.152, 190.34.183.154

SSL/TLS Diffie-Hellman Modulus <= 1024 Bits (Logjam)

Descripción

El host remoto permite conexiones SSL / TLS con uno o más módulos Diffie-Hellman menores o iguales a 1024 bits.

Solución

Reconfigure el servicio para usar un único módulo Diffie-Hellman de 2048 bits o

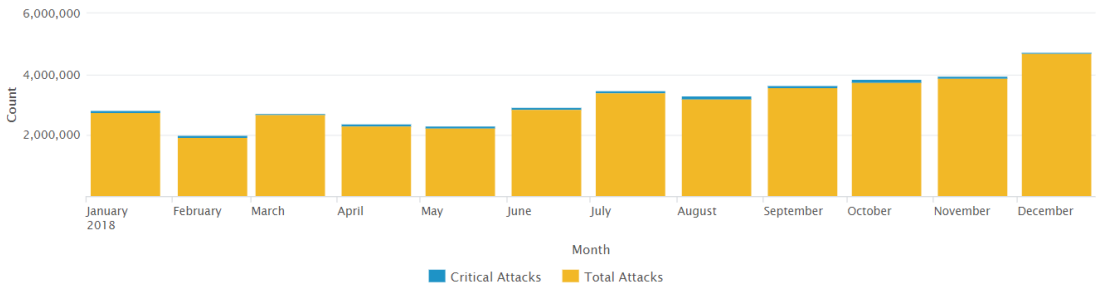
Sistemas Afectados

443 / tcp / possible_wls190.34.183.154, 190.34.183.152, 190.34.183.139

AMENAZAS

GLESEC utiliza sus MSS-APS, MSS-EPS, MSS-SIEM, MSS-EDR y MSS-UTM para determinar actividad de inteligencia de amenazas.

Las Amenazas tal como fueron reportadas por MSS-APS, MSS-APFW para este mes son ataques de Anti-scanning principalmente (escaneos de puertos).



Basándonos en la información recolectada por las contramedidas de seguridad durante este periodo indica 4,702,174 ataques hacia Metrobank S.A.; 44,344 de los cuales fueron considerados "críticos".

Pudimos observar un aumento en actividad de ataques con respecto al mes de diciembre (Ataques totales: 3,874,244) de un 21% aproximadamente y una disminución en ataques críticos con relación al mes de diciembre (Ataques críticos: 87,586) de alrededor de un 49%.
El tipo de ataque crítico que ocurrió con más frecuencia este mes fue Network Flood IPv4 UDP (82%) y pertenece a la categoría Behavorial-DoS.

Durante el mes de diciembre, el servicio MSS-APFW registró un pico de ataques el día 12 de diciembre provenientes de la dirección IP 154.59.121.139 principalmente.

Estos ataques fueron dirigidos en su mayoría a la aplicación "Govimar1", los paquetes enviados estaban forjados para intentar explotar vulnerabilidades de existir dichas vulnerabilidades en el sistema destino. En estos ataques se intentaban explotar vulnerabilidades a través de los puertos 443, 8443 y 80, adicionalmente se

detectó un bajo porcentaje de intentos de SQL Injection (10 intentos).

Todos los ataques mencionados fueron bloqueados por el MSS-APFW.

Ataques Bloqueados de Severidad Critica:

- Network Flood IPv4 UDP (79%), SIP-Scanner-SIPVicious (7.6%).
- Network flood IPv4 TCP-SYN.
- BO-CA-BrighStor-DiscSVC-UDP (22%).
- SQL-Inj-select (3%).

De tipo informativo están los ataques de tipo Anomaly-SSL-renegotiation-Cli que pertenece a la categoría de intrusion en el host 190.34.183.142 hacia el puerto 443.
Entre los ataques frecuentes y bloqueados por semana tenemos: TCP Scanning (Horizontal), TCP Scan, Threat List, Network Flood IPv4 UDP, UDP Scan (horizontal), UDP Scan, SIP-Scanner-SIPVicious, Ping Sweep, TCP Protocol violation, First packet not synchronized y Invalid IP header or invalid total length.
Todo esto fue detenido por las contramedidas de seguridad gestionadas de GLESEC.

La duración que presenta la mayoría de los ataques son:

- Menos de un minuto: de las categorías de Anti-Scanning, Behavioral-DoS and HttpFlood.
- De uno a cinco minutos: de las categorias de Anti-Scanning, Cracking Protection y Behavioral-DoS

Las fuentes de los ataques más frecuentes son los siguientes países: Ucrania (34%), Federación Rusa (19%), Panamá (12%) y Estados Unidos (11%).
Estos están destinados principalmente a múltiples puertos, entre ellos 8545 (JSON RPC, utilizado comúnmente para comunicaciones de la criptomoneda Ethereum) puerto, 23 (telnet) y 445 (SMB).

GLESEC recomienda no utilizar el protocolo telnet para comunicaciones debido a

que toda la información se envía en texto plano, utilizar SSH en su lugar y restringir el acceso al puerto 23. Debido a que hay un número de conexiones dirigidas al puerto 8545 y este puerto es usado en comunicaciones de criptomonedas, es recomendable bloquear el acceso externo a este puerto si no es necesario para el funcionamiento de aplicaciones.

La mayoría de los ataques parecen ser de reconocimiento (Scanning) duraron menos de un minuto y seguidamente de 1 a cinco minutos.

Alrededor de un 95% de los ataques de este mes fueron provenientes de escaneos que pueden considerarse reconocimiento (reconnaissance) y se utiliza como planificación para futuros ataques.
Los ataques que consumen la mayor cantidad de ancho de banda son los ataques de Behavorial-DoS, Anti-Scanning, Access, Anomalies and Intrusions.

El dispositivo DefensePro protege estos ataques dirigidos a la red y en el nivel del servidor dirigido a números de puerto conocidos: 8545 (JSON-RPC), 23 (Telnet), 445 (SMB), 81(HTTP-Alternative), 3389 (RDP), 8080, 1433 (Microsoft SQL), 22(SSH), 443 (HTTPS) en orden de frecuencia para este periodo.

Las 5 principales IP de origen (locales o públicas).

- 190.34.192.73
- 190.34.192.31
- 92.53.64.27
- 176.119.4.53
- 176.119.4.56

Los tipos de ataques más frecuentes fueron TCP Scan y TCP Scan (Horizontal).
La primera y segunda dirección IP fueron los principales atacantes y provienen de Panamá, la tercera dirección IP proviene de la Federación Rusa, la cuarta y quinta direcciones provienen de Ucrania.

Correlación entre los servicios MSS-APS y el MSS-VME

En la siguiente tabla se describe los host críticos del cliente Metrobank S.A que reciben ataques (MSS-APS/APFW) y si estos sistemas tienen vulnerabilidades (MSS-VME).

Destino de ataques (MSS-APS/APFW)	Taques más Frecuentes (MSS-APS/APFW)	N° Ataques	Vulnerabilidades Presentes (MSS-VME)
190.34.183.132 (Check Point)	• Network flood IPv4 UDP (14,255) • Threat List (312) • TCP handshake violation, first packet not syn (70)	14,661	MS15-034: Vulnerability in HTTP.sys Could Allow Remote Code Execution (3042553) (uncredentialed check)
190.34.183.135	• Network flood IPv4 UDP (6,074) • TCP handshake violation, first packet not syn (3,395) • Threat List (328)	10,167	None
190.34.183.158	• Network flood IPv4 UDP (6,675) • TCP handshake violation, first packet not syn (2,631) • Threat List (274)	9,778	None

190.34.183.149 (Exchange)	• Web Scan (2,437) • TCP handshake violation, first packet not syn (1,443) • TCP Scan vertical (397)	4,927	• Microsoft Exchange Client Access Server Information Disclosure • SSL DROWN Attack Vulnerability (Decrypting RSA with Obsolete and Weakened encryption) • SSL Medium Strength Cipher Suites Supported • SSL RC4 Cipher Suites Supported (Bar Mitzvah) • SSL Version 2 and 3 Protocol Support • SSLv3 Padding Oracle On Downgraded Legacy Encryption Vulnerability (POODLE) • Web Server HTTP Header Internal IP Disclosure
190.34.183.137	• Network flood IPv4 UDP (2,194) • TCP handshake violation, first packet not syn (1,552) • Threat List (305) •	4,119	None

190.34.183.154 (Ebanking)	• HTTP Page Flood Attack (932) • TCP handshake violation, first packet not syn (754) • Threat List (325) • Anomaly-SSL-renegotiation-Cli (176) • TCP Scan (Vertical) (134)	2,367	• SSL Anonymous Cipher Suites Supported • SSL Medium Strength Cipher Suites Supported • SSL RC4 Cipher Suites Supported (Bar Mitzvah) • SSL Version 2 and 3 Protocol Support • SSL Weak Cipher Suites Supported • SSL/TLS Diffie-Hellman Modulus <= 1024 Bits (Logjam) • SSL/TLS EXPORT_DHE <= 512-bit Export Cipher Suites Supported (Logjam) • SSL/TLS EXPORT_RSA <= 512-bit Cipher Suites Supported (FREAK)
190.34.183.153 (Ebanking)	• Web Scan (1,914) • Threat List (307) • TCP Scan (vertical) (147)	2,199	None

Análisis:

La mayoría de los ataques en los hosts 190.34.183.132, 190.34.183.135 y 190.34.183.158 fueron network Flood usando el protocolo UDP, estos ataques no apuntan a ninguna vulnerabilidad específica.

- La mayoría de los ataques en host 190.34.183.149 se dividen entre Web Scan, TCP handshake violation y TCP Scan (vertical).
  La exploración web se refiere a una táctica utilizada para recopilar información sobre el servidor, las herramientas automatizadas se utilizan

para enviar diferentes tipos de solicitudes HTTP y analizar las respuestas que obtiene. Estos ataques apuntan a los puertos 80 y 443 y las vulnerabilidades presentes en este host pueden ser explotadas a través de estos puertos.
Las listas de amenaza se refieren al tráfico denegado debido a una coincidencia con una ACL.
TCP Scan (Vertical) se refiere a la práctica de escanear múltiples puertos en un solo host, esta práctica se usa como una táctica de reconocimiento para identificar los puntos débiles en los hosts.

USA-ARGENTINA-PANAMA
México-Perú-Brasil- Chile

Tel: +1 609-651-4246
Tel: +507-836-5355

Info@glesec.com
www.glesec.com