REPORTE DE OPERACIONES E INTELIGENCIA TECNICO DE CIBERSEGURIDAD

BANVIVIENDA

Noviembre 2018

CONFIDENCIAL

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

Info@glesec.com
www.glesec.com

Tabla de contenido

Acerca de este reporte

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. GESEC procesa una gran cantidad de datos y no se puede presentar 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.

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

Servicio Administrado de Vulnerabilidades (MSS-VM)

El Servicio Administrado de Vulnerabilidades (MSS-VM) permite a las organizaciones minimizar los riesgos de las vulnerabilidades mediante la rápida detección de debilidades, midiendo el riesgo potencial y la exposición, generar alertas, proveer información de remediación necesaria para mitigar estos riesgos de forma regular y facilitando el reporte de desviaciones y el cumplimiento con las regulaciones y mejores prácticas.

Definiendo sistemas críticos

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

Host	Sistema o servicio	Observación
200.46.19.100	Banca en línea	Atención a clientes
200.46.227.227	Internet Colaboradores - VPNs	
200.46.227.230	ChatGenesys	Atención a clientes
200.46.227.233	IPS – Admin – VPN	
200.90.137.83	FTP Server	
200.90.137.84	Web Server	Página web
200.90.137.94	Webmail.banvivienda.com – OWA - Exchange	Correo electrónico

Para este periodo y según el rango de direcciones IP proporcionado por BANVIVIENDA se han analizado 12 hosts, de los cuales 9 se encuentran vulnerables. Estas vulnerabilidades se dividen en las siguientes severidades como se muestra en la siguiente tabla. Además, puede observar la Métrica de Valor de riesgo de su organización de acuerdo con nuestras métricas.

Total de IPs Escaneadas				IPs Vulnerables
12				9
Distribución de riesgo				
Critíco	Alto	Medio	Bajo	Total
0	4	23	7	34

Según las mérticas:

RV= 0.335294118

Los siguientes valores son para aclarar el RV:

RV=1 Apunta a todas las direcciones IP en la infraestructura son susceptibles a ataques

RV=0 Apunta a que ninguna dirección IP en la infraestructura es susceptible a ataques

RV=0.1 Apunta a 1/10 de dirección IP en la infraestructura que es susceptible a ataques

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

Category	Critical	High	Medium	Low	Total
General		0	21	7	28
Service detection		4	0	0	4
Misc.		0	1	0	1
Windows		0	1	0	1

- General
- Detección de servicios
- Misceláneos
- Windows

Para el mes de noviembre, se analizarán un total de 12 hosts, de los cuales 9 son vulnerables. BANVIVENDA presenta un total de 34 vulnerabilidades las cuales se dividen de la siguiente manera: 4 vulnerabilidades de riesgo, 23 vulnerabilidades de riesgo medio y 7 vulnerabilidades de riesgo bajo. No se han encontrado vulnerabilidades de riesgo critico en su organización.

A continuación, se muestran las categorías más vulnerables:

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

- **GENERAL** (82.3%) algunas de las vulnerabilidades que se presenta son de tipo:

Valor	Cantidad	Severidad
SSL Medium Strength Cipher Suites Supported	5	Media
SSL RC4 Cipher Suites Supported (Bar Mitzvah)	5	Baja

- **Service Detection** (11.7%) presenta solamente la vulnerabilidad de tipo:

Valor	Cantidad	Severidad
SSL Version 2 and 3 Protocol Detection	4	Alta

- **MISC.** (2.94%) solo presenta la vulnerabilidad de tipo:

Valor	Cantidad	Severidad
SSL DROWN Attack Vulnerability (Decrypting RSA with Obsolete and Weakened eNcryption)	1	Media

- **WINDOWS** (2.94%) la única vulnerabilidad que se presenta es de tipo:

Valor	Cantidad	Severidad
Microsoft Exchange Client Access Server Information Disclosure	1	Media

Para este periodo continúa presentándose la vulnerabilidad severidad alta del tipo SSL Version 2 and 3 Protocol Detection en los hosts 200.90.137.87, 200.90.137.89, 200.46.19.100 y 200.46.227.230 (tienen puertos 443, 25, 10000 y 500 vulnerables), y pertenece a la categoría de service detection.

Principales hosts vulnerables para este período: 200.90.137.87, 200.90.137.89, 200.46.227.230, 200.90.137.91, 200.90.137.94 y 200.46.19.100. La mayoría de estos hosts son vulnerables por el protocolo TCP, a excepción de los hosts 200.46.19.98 y 200.46.227.277 que muestran una vulnerabilidad en el protocolo UDP.

Los puertos más vulnerables para este período son:

- 443 (https) la mayoría de los hosts son vulnerables por este puerto, entre ellos tenemos: 200.46.227.230, 200.90.137.91, 200.46.19.100 y 200.90.137.94.

- 25 (smtp) los 2 hosts vulnerables por este puerto son: 200.90.137.87 y 200.90.137.89.

- 10000 (ndmp), el único host vulnerable para este puerto es 200.90.137.91 y tiene las siguientes vulnerabilidades SSL Certificate Cannot Be Trusted, SSL Certificate Signed Using Weak Hashing Algorithm and SSL Self-Signed Certificate.

- 500 (Ipsec) los 2 hosts vulnerables por este puerto son: 200.46.19.98 y 200.46.227.277 tienen una vulnerabilidad de tipo Microsoft Exchange Client Access Server Information Disclosure.

Entre las vulnerabilidades más frecuentes para este periodo tenemos:

- SSL Medium Strength Cipher Suites Supported
- SSL RC4 Cipher Suites Supported (Bar Mitzvah)
- SSL Certificate Cannot Be Trusted
- SSL Version 2 and 3 Protocol Detection
- SSL Certificate Signed Using Weak Hashing Algorithm
- SSL Self-Signed Certificate
- Internet Key Exchange (IKE) Aggressive Mode with Pre-Shared Key

Lo más recomendable sería reforzarlos, puede encontrar más información sobre ellos en la sección de inteligencia para MSS-VM.

Descripción por Host

Actualmente se siguen presentando la mayoría de las vulnerabilidades que el mes anterior:

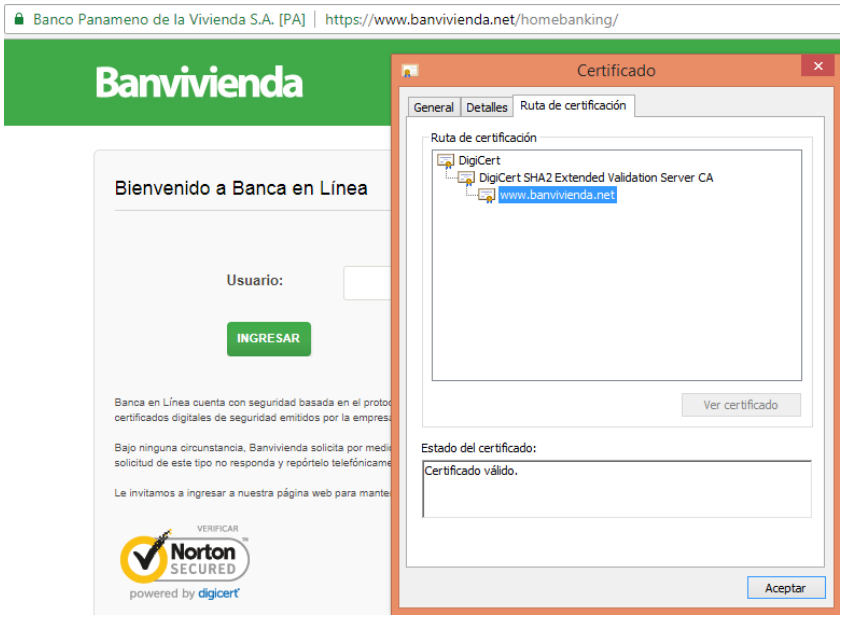
Los siguientes hosts **200.90.137.89** y **200.90.137.87** presentan las mismas vulnerabilidades:

Varias vulnerabilidades encontradas en estos hosts se indican aquí:
SSL Certificate Cannot Be Trusted, SSL Certificate Signed Using Weak Hashing Algorithm, SSL Medium Strength Cipher Suites Supported, SSL Self-Signed Certificate, SSL Version 2 and 3 Protocol Detection, SSL Weak Cipher Suites

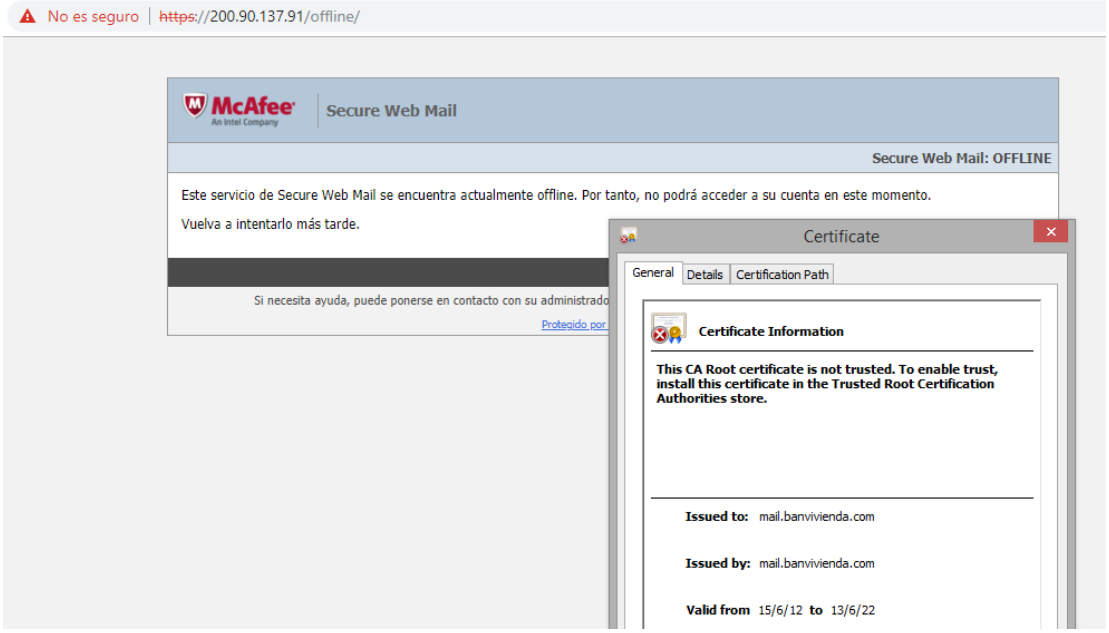
Supported, OpenSSL AES-NI Padding Oracle MitM Information Disclosure, SSL RC4 Cipher Suites Supported (Bar Mitzvah).
Recomendamos seguir el procedimiento de solución para estos problemas, descrito en la sección Vulnerabilidades por gravedad de este documento.

200.46.227.230 (https://www.banvivienda.com/es)
Varias vulnerabilidades encontradas en ese host se indican aquí:
SSL Medium Strength Cipher Suites Supported, SSL RC4 Cipher Suites Supported (Bar Mitzvah), SSL Version 2 and 3 Protocol Detection and SSL Weak Cipher Suites Supported. Recomendamos seguir el procedimiento de solución para estos problemas, descrito en la sección Vulnerabilidades por gravedad de este documento.

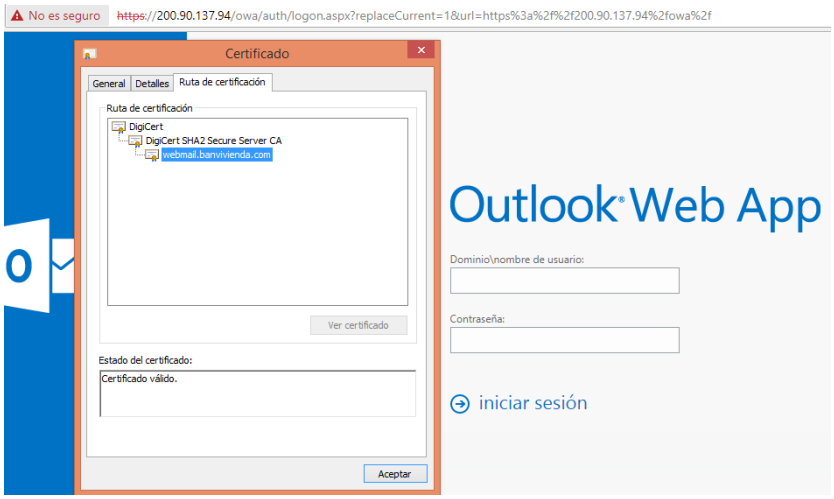
200.46.19.100 (https://www.banvivienda.net/homebanking/)
Varias vulnerabilidades encontradas en ese host se indican aquí:
SSL Version 2 and 3 Protocol Detection, SSLv3 Padding Oracle On Downgraded Legacy Encryption Vulnerability (POODLE), SSL RC4 Cipher Suites Supported (Bar Mitzvah). Recomendamos seguir el procedimiento de solución para estos problemas, descrito en la sección Vulnerabilidades por gravedad de este documento.



200.90.137.91 (https://200.90.137.91/offline/)
Varias vulnerabilidades encontradas en ese host se indican aquí:
SSL Certificate Cannot Be Trusted, SSL Certificate Signed Using Weak Hashing Algorithm, SSL Self-Signed Certificate. Recomendamos seguir el procedimiento de solución para estos problemas, descrito en la sección Vulnerabilidades por gravedad de este documento.



200.90.137.94
(https://200.90.137.94/owa/auth/logon.aspx?replaceCurrent=1&url=https%3a%2f%2f200.90.137.94%2fowa%2f)
Varias vulnerabilidades encontradas en ese host se indican aquí:
Microsoft Exchange Client Access Server Information Disclosure, SSL Medium Strength Cipher Suites Supported, SSL RC4 Cipher Suites Supported (Bar Mitzvah). Recomendamos seguir el procedimiento de solución para estos problemas, descrito en la sección Vulnerabilidades por gravedad de este documento.



Los hosts **200.46.19.98** y **200.46.227.227** tienen la siguiente vulnerabilidad: Aggressive Internet Key Interchange Mode (IKE) with pre-shared key". Recomendamos seguir el procedimiento de solución para estos problemas, descrito en la sección Vulnerabilidades por gravedad de este documento.
De los ataques realizados a su organización, el 94% va específicamente al host 200.46.227.277 y el 6% va al host 200.46.19.98.

Vulnerabilidades por severidad

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

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 varias fallas criptográficas, que incluyen:

- Un esquema de relleno inseguro con cifrados CBC.

- Esquemas inseguros de renegociación y reanudación de sesiones.

Un atacante puede explotar estas fallas para realizar ataques de intermediarios o para descifrar las comunicaciones entre el servicio afectado y los clientes.

Si bien SSL / TLS tiene un medio seguro para elegir la versión con mayor compatibilidad del protocolo (de modo que estas versiones solo se utilizarán si el cliente o el servidor no admiten nada mejor), muchos navegadores web implementan esto de una manera insegura que le permite a un atacante degradar una conexión (como en POODLE). Por lo tanto, se recomienda que estos protocolos estén completamente desactivados.

Solución
Consulte la documentación de la aplicación para deshabilitar SSL 2.0 y 3.0.
Utilice TLS 1.1 (con conjuntos de cifrado aprobados) o superior en su lugar.

Sistemas Afectados
25 / tcp / smtp 200.90.137.87, 200.90.137.89.
443/tcp/ possible_wls 200.46.19.100, and 200.46.227.230.

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 utiliza longitudes de clave de al menos 64 bits y menos de 112 bits, o bien que utiliza el conjunto de cifrado 3DES.

Tenga en cuenta que es considerablemente más fácil evitar el cifrado de intensidad media si el atacante está en la misma red física.

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

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

Sistemas Afectados
25 / tcp / smtp 200.90.137.87, 200.90.137.89

Affected Systems
443 / tcp / possible_wls 200.46.227.230, 200.46.227.230, 200.90.137.94, 200.90.137.94

SSL Certificate Signed Using Weak Hashing Algorithm

Description
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 que caducan después del 1 de enero de 2017 como vulnerables. Esto está de acuerdo con la puesta en marcha gradual de Google del algoritmo hash criptográfico SHA-1.

Sistemas Afectados
25 / tcp / smtp 200.90.137.87200.90.137.89
443 / tcp / possible_wls 200.46.227.230, 200.46.227.230
443 / tcp / possible_wls 200.90.137.91
10000 / tcp / possible_wls 200.90.137.91

SSLv3 Padding Oracle On Downgraded Legacy Encryption Vulnerability(POODLE)

Description
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).
Los atacantes de MitM pueden descifrar un byte seleccionado de un texto cifrado en

tan solo 256 intentos si pueden forzar a una aplicación víctima a enviar repetidamente los mismos datos a través de las conexiones SSL 3.0 recién creadas.

Solución
Desactivar SSLv3.

Sistemas Afectados
443 / tcp / www 200.46.19.100

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.

Si el texto simple se cifra repetidamente (por ejemplo, las cookies HTTP), y un atacante puede obtener muchos textos cifrados (es decir, decenas de millones), el atacante puede derivar el texto simple.

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
25 / tcp / smtp 200.90.137.87, 200.90.137.89
443 / tcp / possible_wls 200.90.137.94
443 / tcp / possible_wls 200.46.19.100
443 / tcp / possible_wls 200.46.227.230

OpenSSL AES-NI Padding Oracle MitM Information Disclosure

Descripción

El host remoto se ve afectado por una vulnerabilidad de divulgación de información de man-in-the-middle (MitM) debido a un error en la implementación de conjuntos de cifrado que utilizan AES en modo CBC con HMAC-SHA1 o HMAC-SHA256.

La implementación está especialmente escrita para utilizar la aceleración AES disponible en los procesadores x86 / amd64 (AES-NI). Los mensajes de error devueltos por el servidor permiten que un atacante de tipo "man in the middle" realice un ataque de oráculo de relleno, lo que da como resultado la capacidad de descifrar el tráfico de la red.

Solución

Actualice a la versión 1.0.1t / 1.0.2h o posterior de OpenSSL..

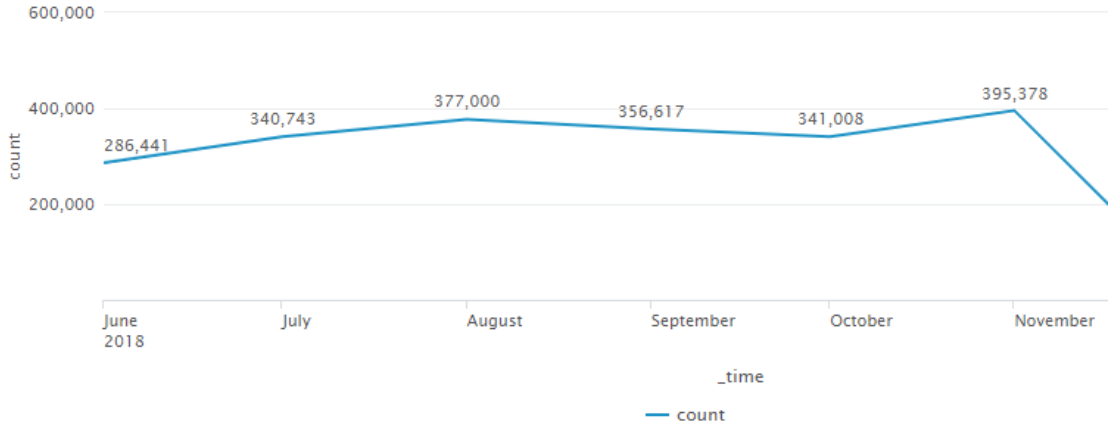
Sistemas Afectados

25 / tcp / smtp 200.90.137.87, 200.90.137.89

Amenazas

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

Las amenazas informadas por MSS-APS, MSS-EPS, MSS-SIEM, MSS-EDR, MSS-UTM para este mes, hay un total de **395,378** ataques denegados por las reglas del firewall.



En base a la información recopilada de las medidas de seguridad durante este mes, todos los intentos de acceso para BANVIVIENDA fueron bloqueados por las reglas de ACL configuradas. Las diferentes fuentes de direcciones IP envían paquetes de tipo ICMP, UDP y TCP a los hosts 200.46.227.227 (85.2%) y 200.46.19.98 (14.7%). Explore una cantidad significativa de ataques que pueden considerarse reconocimiento por ataques posteriores, le recomendamos que verifique la actividad de los dispositivos donde se registran estos eventos.

Entre los 5 principales países que frecuentan el mayor número de ataques están:

País	Cantidad
• China	6,114
• Estados Unidos	4,395
• Rusia	3,841
• Brasil	1,994
• Panamá	1,503

Para este período, el total de eventos de seguridad para CISCO ASA fue: 1,634,803; que se dividen de la siguiente manera: 1,276,288 se registraron en el host

200.46.19.98 y 358,515 se registraron en el host 200.46.227.227.
En la siguiente lista podemos ver las acciones que fueron bloqueadas por las reglas de ACL y los ataques que se registraron en cada una de ellas:

Acción	Cantidad	Tipo de Ataque
• Deny	174,519	ANTI-SPOOF
• Connection deny	141,666	TCP CHECK
• Access denied	54,668	-
• Deny Inbound	6,899	UDP CHECK, ICMP CHECK, DNS SNOOP, L3 DROP
• Dropping	900	MGMT PLANE

Entre las actividades de red más frecuentes se encuentran: Network Access Point, IKE and IPsec, User Session, Access Lists, IP Stack y NAT and PAT.

Tipos de ataques presentados durante este mes:

A continuación, se muestran los ataques más frecuentes y la cantidad que se registró en cada uno de ellos.

Tipo de ataque	Cantidad
• ANTI-SPOOF	174,519
• TCP CHECK	141,666
• UDP CHECK	5,657
• MGMT PLANE	900
• ICMP CHECK	911
• DNS SNOOP	310
• L3 DROP	21

Intentos de ataque bloqueados hacia un puerto de destino específico

En esta sección, muestra una lista de los puertos atacados durante este período se enumeran en orden descendente donde el primer puerto fue el que recibió la mayoría de los ataques.

- HTTP (80)
- TELNET (23)

- SSH (22)
- HTTPS (443)
- SNMP (161)

El puerto 80 recibió aproximadamente un 48% de los ataques que fueron bloqueados.

Las cinco principales fuentes de IP (locales o públicas)

La dirección IP privada aparece en esta sección porque el dispositivo de contramedidas de seguridad ha denegado la conexión TCP a otro dispositivo interno, esto puede suceder debido a configuraciones erróneas. Las IP públicas se destacan para un reconocimiento más rápido

- 10.100.201.45
- 200.46.3.93
- 104.248.119.106
- 117.10.51.192
- 200.46.73.116

Las direcciones 200.46.73.116 y 104.248.119.106 también estaban en la lista de fuentes principales registradas en el mes de octubre.

Los cinco principales IP de destino (locales o públicos)

En esta sección presentamos las direcciones IP de destino de las conexiones denegadas o descartadas que fueron más recurrentes durante este período.

- 192.168.1.1
- 200.46.227.227
- 200.46.19.98
- 172.20.10.2
- 10.100.210.133

Servicio de Detección y Respuesta en Dispositivos Finales (MSS-EDR)

El MSS-EDR es un servicio de detección preventiva, respuesta y forense para identificar sin firmas y mitigar un ataque a los puntos finales y servidores de una organización. El servicio funciona buscando activamente actividad maliciosa en la red del cliente en función de comportamientos sospechosos (no basados en firmas). Esta tecnología permite a nuestros analistas detectar software malicioso que puede haber evadido las contramedidas de seguridad existentes. Al mismo tiempo, llevamos a cabo investigaciones respondiendo a una alerta de seguridad: este servicio se basa en aprovechar una poderosa plataforma de investigación para acortar el tiempo de investigación, responder a más incidentes y llegar a la causa raíz de cada incidente.

Las alertas registradas en este mes están relacionadas con fuerza bruta, debido a que los usuarios realizaban una cantidad excesiva de intentos de acceso fallidos al realizar cambios en sus contraseñas. Otras alertas que se registraron en menor cantidad están relacionadas con archivos ejecutables, uno está relacionado con accesos remotos a los sistemas y el otra está relacionada con un script que forma parte de la infraestructura.

Las alertas que se enumeran a continuación provienen de actividades realizadas dentro de su organización (eventos), que representan un nivel de gravedad (crítico, alto, medio, bajo o informativo) de acuerdo con el comportamiento registrado.

El análisis de seguridad realizado dentro de nuestro GOC se centra en detectar amenazas, correlacionar y analizar indicadores en cuatro áreas críticas de su organización: archivos, usuarios, redes y puntos finales.

1. Usuario

Fuerza Bruta

- Entre los usuarios más frecuentes que presentaron esta alerta podemos mencionar: darlene.granizo (45%), Joel.alvarado (18%), Jorge.vergara (10%), deyvis.tejedor (4%) y dora.rosas (4%).

- Se registró un total de 379 eventos.

A continuación, se listan un resumen de los eventos más relevantes relacionados a fuerza bruta para el mes de noviembre.

Incidente detectado			
Fecha	**Hora**	**Usuario**	**Numero de Intentos Fallidos**
1 NOVIEMBRE	08:13	deyvis.tejedor	11
	08:45	Xiomara.dominguez	12
	08:52 – 12:42 (17*)	Darlene.granizo	12
	15:16	Jose.mulino	14
	15:19, 15:24, 16:39, 18:53, 19:13	Darlene.granizo	12
2 NOVIEMBRE	08:29, 09:42		12
	10:16	Joaquin.victoria	38
	10:17	Jose.mulino	12
	12:01, 12:03	Margarita.moreno	17
	12:10, 12:15, 12:50, 13;45	Darlene.granizo	12
	14:09	Deyvis.tejedor	13
	14:10, 14:58, 15:11,	Darlene.granizo	12
	17:54	Deyvis.tejedor	11
	18:13 - 23:04 (9*)	Darlene.granizo	12
3 NOVIEMBRE	00:01	Mercedes.willa	11
	00:50	Darlene.granizo	12
	02:30	Deyvis.tejedor	11
	08:51, 10:01, 13:02, 14:17, 14:23, 15:31	Darlene.granizo	12
	23:53	Deyvis.tejedor	14
4 NOVIEMBRE	09:41, 09:43, 09:58		11
	10:39	Rolando.rojas	12
	14:50 - 20:45 (8*)	Jorge.vergara	12
	20:49, 20:51, 20:54	Darlene.granizo	12
5 NOVIEMBRE	02:08		
	09:31	Jorge.vergara	17

	10:42, 11:12	Darlene.granizo	12
	11:45, 12:36, 12:39,	Jorge.vergara	18
	13:30	Darlene.granizo	12
	15:20, 15:24	Jorge.vergara	14
6 NOVIEMBRE	00:07, 02:30		16
	02:52 - 07:18 (6*)	Darlene.granizo	14
	10:42	Jorge.vergara	13
7 NOVIEMBRE	04:48	Darlene.granizo	11
	06:16, 06:18, 06:20	Dora.rosas	11
8 NOVIEMBRE	00:26, 00:48, 00:51	Darlene.granizo	12
	00:57, 00:58, 09:42, 17:20	Jazmin.perez	12
8 NOVIEMBRE	19:50	Maria.avila	12
	20:05, 22:11, 22:17, 22:59, 23:13	Darlene.granizo	14
9 NOVIEMBRE	01:23 - 21:20 (12*)		14
10 NOVIEMBRE	10:09 - 17:43 (7*)		16
	18:10, 18:15	Jose.mulino	16
	18:46	Darlene.granizo	14
	18:48 – 18:58 (7*), 19:03 – 19:14 (9*)	Joel.alvarado	14
	19:48, 20:49	Darlene.granizo	12
11 NOVIEMBRE	00:02 - 15:13 (9*)		14
12 NOVIEMBRE	11:01, 11:04	Jose.mulino	22
	16:29 - 18:47 (9*)	Joel.alvarado	12
13 NOVIEMBRE	08:03	Darlene.granizo	12
	08:28	Mercedes.willa	16
	18:02 – 18:59 (17*), 19:05 – 19:59 (22*),	Joel.alvarado	16
	21:02	Maria.avila	20
14 NOVIEMBRE	10:13, 12:22	Angeliki.gionis	13
	21:31	Maria.avila	12
15 NOVIEMBRE	10:37	Darlene.granizo	12

	23:03	Dora.rosas	13
16 NOVIEMBRE	13:04, 13:14	Deyvis.tejedor	13
	13:37	Darlene.granizo	12
	14:09	Michelle.harris	11
	17:30	Deyvis.tejedor	11
	22:32	Maria.avila	28
17 NOVIEMBRE	10:49, 12:43	Sandra.valbueno	12
	17:31	Deyvis.tejedor	11
18 NOVIEMBRE	02:50, 06:35		11
	17:48, 18:13, 18:19	Lineth.ruiz	12
19 NOVIEMBRE	02:32, 07:42		12
	07:48	Sandra.valbueno	11
	09:18	Lineth.ruiz	13
	10:57	Michelle.harris	14
	11:20, 13:24, 17:32	Darlene.granizo	12
	19:36	Maria.avila	14
	21:10	Dora.rosas	12
20 NOVIEMBRE	7:47	Alitzka.marin	13
	7:57	Danilka.gonzalez	12
	8:18	Darlene.granizo	12
21 NOVIEMBRE	5:53	Eduardo.alain	15
23 NOVIEMBRE	09:01	Darlene.granizo	12
	19:35		18
24 NOVIEMBRE	18:55	Dora.rosas	11
25 NOVIEMBRE	14:52	Jose.mulino	15
	18:52 - 23:17	Michelle.harris	12
26 NOVIEMBRE	06:13, 10:03		
	13:47, 14:08	Juan.arango	21
	15:53	Michelle.harris	11
27 NOVIEMBRE	08:16	Jorge.gaitan	11
28 NOVIEMBRE	09:26	Darlene.granizo	12
29 NOVIEMBRE	08:25	yehymi.ortega	12
30 NOVIEMBRE	00:02, 00:03, 03:03	Dora.rosas	13

	13:23	Vielka.garcia	11
	17:50, 17:51	Darlene.granizo	12

EL asterisco (*) indica que se registraron esa cantidad de eventos entre esas horas.

El evento de Fuerza Bruta tiene un nivel de severidad alto y se registra en el host BpvExch02.

2. Archivos

Las siguientes tablas mostrarán los archivos que se registraron con comportamiento malicioso:

dwrcs.exe

El software DameWare que permite a un "operador" remoto controlar un sistema como si tuviera acceso físico a ese sistema.

Severidad	Informativa						
Host	BpvUltimusFE84	BPVBLW1	bpvblbe1	bpvblwb2	BPVBLBE2	BpvUltimusFE	BpvUltimusDB84
Fecha	17/11/18	17/11/2018	17/11/2018	17/11/10	17/11/10	17/11/18	17/11/18
Hora	21:36	22:00	22:00	22:17	22:41	23:16	23:57
Path	c:\windows\syswow64\dwrcs.exe						
Md5	A49A04F4A37965790E39E43976B16A43						
Hash	EB30A0075CDC0C3DDEA9B22B92E4D0F275932F9FDCB10B9D4D4BD8B3C03DA0BE						

teamviewer_service.exe

Software que permite a un "operador" remoto controlar un sistema como si tuviera acceso físico a ese sistema.

Severidad	Informativa
Host	BpvMultipagoV12
	Fecha: 17/11/18 21:01

	Path: c:\users\bpvsvradm\appdata\local\temp\1\teamviewer\teamviewer_service.exe
	Hash: 0B16298895E87247CF5C41DA9A812A1F8D680960E8A1F64204C8E8A05883E431
	MD5: AAE6D081A16399B629D7DA227C5ADB6F
	Versión del software: TeamViewer 11.0.15161.0
Host	BPVWebSvr
	Fecha: 18/11/18 18:24
	Path: c:\users\bpvsvradm\appdata\local\temp\2\teamviewer\teamviewer_service.exe
	Hash: E90EEC1C65958873FA7327307184D5155C94D50C59D9869A9EA5834E8CADE4CD
	MD5: 758B320E709CBF1D0C34A18390EEE6E8
	Versión del software: TeamViewer 10.0.43174.0

cmd.exe

Descripción	Host IP: 10.100.210.55
Severidad	**Critica**
Host	BpvUltimusFE84
Fecha	11/20/18 17:17
Path	c:\windows\system32\reg.exe
Hash	6F88FB88FFB0F1D5465C2826E5B4F523598B1B8378377C8378FFEBC171BAD18B
Process Running User	banvivienda\jorge.gaitan
Malicious Command Line	C:\Windows\System32\reg.exe ADD HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\System /v EnableLUA /t REG_DWORD /d 0 /f
Process Params	C:\Windows\system32\cmd.exe /c ""\\Banvivienda.local\SysVol\Banvivienda.local\Policies\{2EC897F1-5BAC-4E9C-8B20-12E6268731C8}\User\Scripts\Logon\UACDisable.bat" "

Descripción	Host IP: 10.100.201.119
Severidad	**Critica**
Host	BpvExch02
Fecha	11/29/18 23:06
Path	c:\windows\system32\reg.exe
Hash	6F88FB88FFB0F1D5465C2826E5B4F523598B1B8378377C8378FFEBC171BAD18B
Process Running User	banvivienda\jorge.jarpa
Malicious Command Line	C:\Windows\System32\reg.exe ADD HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\System /v EnableLUA /t REG_DWORD /d 0 /f
Process Params	C:\Windows\system32\cmd.exe /c ""\\Banvivienda.local\SysVol\Banvivienda.local\Policies\{2EC897F1-5BAC-4E9C-8B20-12E6268731C8}\User\Scripts\Logon\UACDisable.bat" "

- Los eventos con severidad informativa ya fueron notificados al cliente.
- Los eventos con severidad critica relacionados con el script “UACDisable.bat” ha sido reportado anterioridad al cliente, el cual nos indica que este script es aprobado y utilizado por los administradores de infraestructura.

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

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

Info@glesec.com
www.glesec.com