



REPORTE DE OPERACIONES E INTELIGENCIA EJECUTIVO DE CIBERSEGURIDAD

BANVIVIENDA

Octubre 2018

Tel: +1 609-651-4246

Tel: +507-836-5355

Info@glesec.com

www.glesec.com

CONFIDENCIAL

Tabla de contenido

Tabla de contenido	2
Sobre este informe	¡Error! Marcador no definido.
Alcance de este informe	3
Resumen Ejecutivo	¡Error! Marcador no definido.
Recomendaciones	15
Sección de Inteligencia por módulo de servicio.....	16
Operaciones de Ciber Seguridad	30
Definiciones	31

CONFIDENCIAL



Sobre este informe

El propósito de este documento es reportar el “estado” de seguridad de su organización. Debe ser destacado que GLESEC basa el análisis de la información en los servicios contratados. La información generada por estos servicios es luego agregada, correlacionada y analizada. Mientras más completo sea el grupo de servicios contratados, más precisos y completos serán los resultados.

Este Informe se organiza en tres partes; La primera es el Resumen Ejecutivo con recomendaciones (como sean necesarias o aplicables), la segunda es la Sección de Inteligencia, con más información detallada, tableros de análisis y la última es la Sección Operacional, con el estado de los servicios y contramedidas bajo contrato, tickets por cambios de mantenimiento e incidentes reportados y actividad consultada en el mes.

Nosotros en GLESEC creemos que la seguridad de la información es un proceso dinámico y holístico que requiere investigación sobre la marcha y seguimiento y debe ser manejado con las herramientas, sistemas y procesos correctos, así como personal capacitado y dedicación. El proceso es dinámico debido al constante descubrimiento de nuevas vulnerabilidades y exploits, la proliferación de herramientas de hacking que hacen muy fácil para principiantes con mínimo conocimiento causar daño. El incremento en malware, phishing, amenazas internas, espionaje, crimen organizado, robo de propiedad intelectual y hacktivismo son la causa de exposición de la seguridad de la información y son impulsados más comúnmente por una ganancia económica. Los servicios subcontratados de GLESEC, basados en el portafolio de su plataforma propietaria TIP™ proveen la respuesta ideal para lo expuesto anteriormente.

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.

CONFIDENCIAL



Alcance de este informe

Tabla Servicios contratados con GLESEC

Esta tabla en lista los servicios e inteligencia de GLESEC TIP™ que están contratados actualmente y la correspondiente fecha de expiración de estos.

Type	Service	Contracted?	Service Expiration
Threat Mitigation	MSS-APS		
Threat Mitigation	MSS-APS-SSL		
Threat Mitigation	MSS-APS-PS		
Threat Mitigation	MSS-APFW		
Vulnerability Testing	MSS-VME	YES	July 1, 2019
Vulnerability Testing	MSS-VMI		
Compliance	MSS-EPS		
Threat Mitigation	MSS-SIEM	YES	July 1, 2019
Risk assessment	MSS-BAS		
Threat Mitigation	MSS-EDR	YES	July 1, 2019
Threat Mitigation	MSS-UTM		
Threat Mitigation	MSS-INT		
Access Control	MSS-TAS		

CONFIDENCIAL



Resumen Ejecutivo

Este informe corresponde al periodo octubre, 2018.

La siguiente tabla describe las categorías principales que GLESEC ha identificado reportar en el estado-de-seguridad de sus clientes-miembros. Las categorías en la tabla de abajo son basadas en una metodología de manejo de riesgo. Esto es un aspecto principal y fundacional de GLESEC.

	RISK / RIESGO
	VULNERABILITIES / VULNERABILIDADES • MSS-VM Service
	THREATS / AMENAZAS • MSS-APS; MSS-EPS; MSS-SIEM; MSS-EIR; MSS-UTM
	ASSETS / ACTIVOS • MSS-VM; MSS-EPS
	COMPLIANCE / CUMPLIMIENTO • MSS-EPS
	SECURITY VALIDATION / VALIDACION • MSS-BAS
	TRUSTED ACCESS / ACCESS CON CONFIABILIDAD • MSS-TAS

RISK

La Gestión de riesgo es el proceso continuo de identificar, evaluar y responder al riesgo. Para gestionar el riesgo, las organizaciones deben entender la probabilidad que un evento ocurra y el impacto resultante. Con esta información, las organizaciones pueden determinar el nivel aceptable de riesgo para la prestación de servicios y pueden expresar esto como su tolerancia al riesgo. El marco de referencia para Ciberseguridad del NIST.

Una de las columnas fundacionales de GLESEC es basar todas sus actividades en lograr la determinación y mitigación de riesgo. Lo que cualquier organización debería querer conocer es cuál es su nivel de Riesgo, en este caso en particular enfocado en seguridad cibernética. Riesgo en Seguridad tiene un impacto directo en el negocio y, como tal, es de suma importancia para los Directivos y la Administración de la compañía.

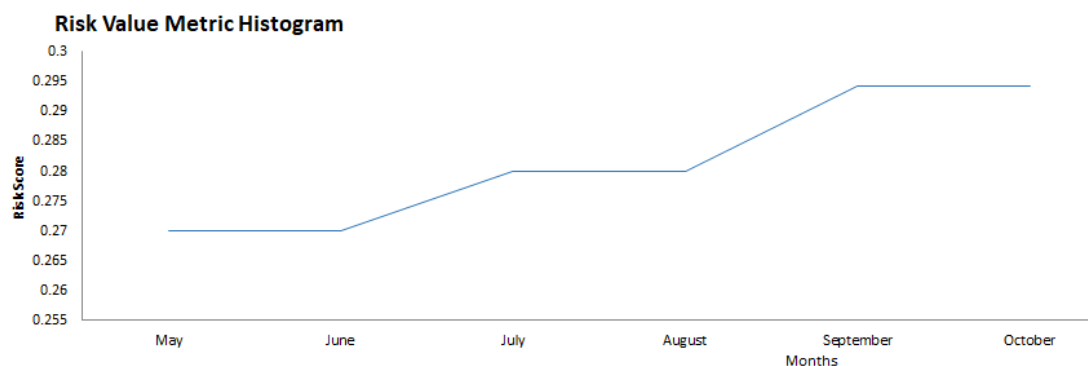
CONFIDENCIAL

Nosotros en GLESEC medimos RIESGO a través de varias perspectivas y utilizando varios de los servicios de la plataforma TIP™. El MSS-VM o Servicio de Seguridad Administrado para Manejo de Vulnerabilidades nos proporciona una vista, cuán débiles son los sistemas de la organización. El MSS-BAS nos proporciona una visión de cuán débiles son las defensas de la organización a las últimas amenazas. El MSS-APS, MSS-SIEM, MSS-UTM, MSS-EDR, MSS-EPS nos proporcionan información de ataque tanto interna como externa, DDOS, Malware, ransomware y otra información vectorial de ataque, así como también brinda servicios de nivel de protección. El MSS-EPS también nos proporciona información de nivel de RIESGO por incumplimiento de los requisitos y / o regulaciones internas o externas. En general, una variedad de servicios nos proporcionan diferentes puntos de vista y juntos tenemos la vista más completa de la postura de seguridad de nuestros clientes.

Determinamos que la condición de riesgo para BANVIVIENDA para el mes de octubre es alta. Esto se puede ver en el indicador de seguridad como se indica a continuación.

Indicador de riesgo	Servicio	Condición	Comentarios
Métrica de Valor de Riesgo	MSS-VME	ALTO	Se reportan 5Mvulnerabilidades de riesgo alto. Cualquiera de estas puede causar un impacto en BANVIVIENDA.

El histograma de MÉTRICA DE VALOR DE RIESGO que se muestra a continuación representa los cambios en la métrica de valor de riesgo basada en vulnerabilidades en los últimos seis meses.



El nivel de riesgo para BANVIVIENDA, durante este periodo del mes es igual al reportado durante el mes de octubre.

Recomendamos para BANVIVIENDA, remediar las vulnerabilidades actuales para tener mayor seguridad en sus sistemas; puede ver una información detallada de las vulnerabilidades por host en nuestro informe técnico mensual.

VULNERABILIDADES

El servicio MSS-VM (E / I) de GLESEC se utiliza para realizar dos pruebas semanales a sistemas externos y / o internos (según las opciones del servicio contratado). De las dos pruebas que se realizan semanalmente, una es una prueba de descubrimiento de los activos en la red y el otro para detectar vulnerabilidades. Las pruebas externas se realizan desde la plataforma en la nube de GLESEC y la interna se realiza con el dispositivo de seguridad múltiple de GLESEC (GMSA).

Las vulnerabilidades son debilidades que, de ser explotadas, pueden comprometer la organización y, como tales, son un componente de RIESGO para la organización. Si hay vulnerabilidades y también amenazas, existe el RIESGO de que la organización puede verse afectada. Las vulnerabilidades informadas por GLESEC deben considerarse todas importantes y abordarse según la prioridad (crítica, alta, media y baja). Un proceso efectivo es trabajar con la información proporcionada por GLESEC y el equipo de consultoría GLESEC para abordar las recomendaciones proporcionadas de manera sistemática y continua. El progreso puede ser determinado por las pruebas semanales.

Según el rango de direcciones proporcionado por BANVIVIENDA, para este período el número total de hosts analizados fue de 15, de los cuales 10 son vulnerables. El número total de vulnerabilidades encontradas fue de 40, que se clasifican como 5 (11,1%) de alto riesgo, 26 (66,7%) de riesgo medio y 9 (22,2%) de bajo riesgo. No se encontraron vulnerabilidades de riesgo crítico.

La vulnerabilidad de riesgo alto de tipo Detección de protocolos SSL versión 2 y 3, todavía está presente en los hosts: 200.46.227.230, 200.46.19.100, 200.90.137.89 y 200.90.137.87.

Entre las principales categorías con mayor número de vulnerabilidades, podemos mencionar:

Valor	Cantidad	
• General	28	77.7%
• Detección de Servicio	4	11.1%
• Misceláneo	3	8.3%



- Windows 1 2.7%

Principales 5 hosts vulnerables:

- 200.90.137.87
- 200.90.137.89
- 200.46.227.230
- 200.46.19.100
- 200.90.137.91

Los puertos más vulnerables en estos hosts son: 443, 25, 10000 y 500; la mayoría de estos puertos tienen un nivel de severidad medio.

Las vulnerabilidades de riesgo media más comunes son:

- Suites de cifrado de fortaleza media soportado
- Certificado SSL no puede ser de confianza
- Certificado SSL firmado con un algoritmo de hash débil
- Certificado autofirmado SSL
- Se admiten suites de cifrado débil SSL
- Internet Key Exchange (IKE) Modo Agresivo con Llave
- SSLv3 Padding Oracle On Vulnerabilidad de cifrado heredado degradado (POODLE)
- Divulgación de información del servidor de acceso de cliente de Microsoft Exchange

Métrica de Valor de Riesgo

GLESEC utiliza una métrica para proveer una manera de cuantificar las vulnerabilidades basada en riesgo de la organización. Esta métrica mide el valor relativo de las vulnerabilidades y también el registro de cambio a través del tiempo.

Es importante mencionar que esta métrica considera media de las vulnerabilidades clasificadas como “críticas”, “alto”, “medio” y “bajo”, dándoles un peso de 100%, 75%, 50% y 10% respectivamente.

Esto toma en consideración todas las vulnerabilidades, pero es importante destacar que estos valores (100%, 75%, 50% y 10%) son arbitrariamente escogidos por nosotros, por lo cual pueden cambiar con el tiempo como resultado de comprender mejor los riesgos involucrados. Podemos usar esta métrica para evaluar el progreso en el tiempo y comparar uno con el otro utilizando un conjunto de cantidad común.



REPORTE PARA:

BANVIVIENDA

Los siguientes rangos de redes externas 200.46.227.224/28, 200.90.137.80/28, 200.46.80.104/29, 200.46.19.96/29 para BANVIVIENDA fueron analizados en busca de vulnerabilidades.

La siguiente tabla indica la métrica de vulnerabilidades externas.

Total IP's Scanned				IP's Vulnerable	
15				10	
Risk Distribution					
Critical	High	Medium	Low	Total	
0	5	26	9	40	

According to the metrics:

RV= 0.294166667

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

Listado externo de vulnerabilidades por condición:

Vulnerable Hosts	Critical	High	Medium	Low	Total
200.46.19.98		0	1	0	1
200.46.19.100		1	1	1	3
200.46.227.227		0	1	0	1
200.46.227.230		1	4	1	6
200.90.137.83		0	1	0	1
200.90.137.84		0	1	1	2
200.90.137.87		1	5	2	8
200.90.137.89		1	5	2	8
200.90.137.91		0	3	0	3
200.90.137.94		0	2	1	3

La siguiente tabla provee una comparativa de las vulnerabilidades externas persistentes del mes actual con respecto al mes pasado.

CONFIDENCIAL



REPORTE PARA:

BANVIVIENDA

host-ip	Previous Month	Current Month
200.46.19.100	3	3
200.46.19.98	1	1
200.46.227.227	1	1
200.46.227.230	6	6
200.90.137.83	5	1
200.90.137.84	2	2
200.90.137.87	8	8
200.90.137.89	8	8
200.90.137.91	3	3
200.90.137.94	3	3

Por favor referirse a las recomendaciones para más detalles. Estas pueden ser vistas en el GLESEC MEMBER PORTAL (GMP).

Categorías de vulnerabilidades

La siguiente tabla indica las categorías que nosotros usamos para vulnerabilidades como una manera de proveer contexto a las mismas y facilitar la priorización de cómo manejar la remediación.

Preliminary Analysis	Firewalls	Network Devices
SMB/NetBIOS	SSH Servers	Malformed Packets
Simple Network Services	Mail Servers	Proxy Servers
Policy Checks	SQL Servers	Wireless AP
Web Servers	FTP Servers	Webmail Servers
RPC Services	Server Side Scripts	NFS Services
Backdoors	SNMP Services	Printers
Encryption and Authentication	DNS Servers	

Basado en lo anterior, la siguiente tabla muestra una matriz del total de vulnerabilidades externas por categoría.

Category	Critical	High	Medium	Low	Total
General		0	21	7	28
Service detection		4	0	0	4
Misc.		0	2	1	3
Windows		0	1	0	1

AMENAZAS

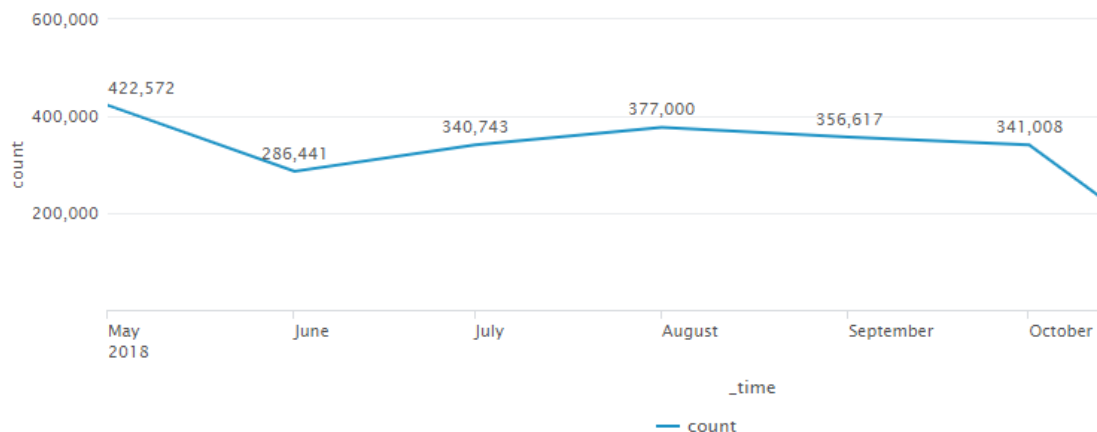
GLESEC utiliza sus MSS-APS, MSS-EPS, MSS-SIEM, MSS-EDR y MSS-UTM para

CONFIDENCIAL



determinar actividad de inteligencia de amenazas.

Las amenazas informadas por MSS-APS, MSS-EPS, MSS-SIEM, MSS-EDR y MSS-UTM para este mes, hay un total de **341,008** ataques denegados por las reglas del firewall.



Para este mes hubo una disminución del 4,37% en la actividad de ataque, en comparación con el mes de septiembre.

Todos los intentos de acceso fueron bloqueados por las reglas de ACL configuradas; diferentes direcciones IP envían paquetes ICMP, UDP y TCP; Principalmente a los siguientes hosts 200.46.227.227 y 200.46.19.98. Analice un número significativo de ataques que pueden considerarse reconocimiento, para ataques posteriores.

Recomendamos a BANVIVIENDA revisar la actividad de los dispositivos donde se registran estos eventos.

Las fuentes de los ataques provienen de los siguientes países: China, Rusia, Estados Unidos, Brasil y Panamá.

Durante este mes, las direcciones a las que se han denegado los intentos de acceso son:

- 200.46.73.116
- 10.100.201.49
- 104.248.119.106
- 104.248.67.229
- 200.46.136.31
- 37.49.231.58

Algunos de los puertos de destino más específicos son: 23 (telnet), 80 (http), 443 (https), 22 (ssh) y snmp.

Entre las actividades de red más frecuentes están: Punto de acceso a la red, IKE e IPsec, Sesión de usuario, Listas de acceso, Pila de IP, NAT y PAT, Alta disponibilidad (Failover) e Interfaz de comandos, que se notaron durante el mes.

Principales 5 equipos monitoreados de BANVIVIENDA durante este mes:

- 200.46.227.227
- 200.46.19.98
- 172.20.15.43
- 172.16.99.99
- 172.16.78.15

ACTIVOS

El MSS-VM(E/I), MSS-EPS realiza una prueba semanal. El MSS-VM(E/I) identifica activos dentro de la red mientras que el MSS-EPS identifica aplicaciones. Dependiendo de los servicios contratados, es la lista que se puede proporcionar de los activos del sistema o aplicativos.

Creemos que no podemos proteger lo que no sabemos y conocer los activos (sistemas y aplicaciones) es fundamental para tener una buena práctica de seguridad cibernética. Por lo tanto, le recomendamos que verifique la información que proporcionamos y que nos haga saber si algo es sospechoso o simplemente no está bien. Podemos trabajar con su organización para crear una línea base que se pueda usar para identificar desviaciones. Por favor, póngase en contacto con nuestro GOC para obtener ayuda en este tema.

El siguiente histograma muestra el total de sistemas descubiertos en el perímetro de su organización en los últimos seis meses.

CONFIDENCIAL





Como puede ver, el número de hosts analizados no cambiado en comparación a los últimos meses.

Saber qué hay en tu red es extremadamente importante. Nuestro equipo de monitoreo en nuestro GOC ha estado investigando todos estos resultados de descubrimiento de host y no ha encontrado nada inusual.

CUMPLIMIENTO

El MSS-EPS o Managed End Point Security Service es un servicio de cumplimiento y remediación. Por cumplimiento entendemos el monitoreo, pruebas y alertas de las desviaciones de los parámetros de todos los “equipos” y “servidores” en la organización con respecto a las líneas base establecidas. Estas líneas base puede ser creadas para soportar requisitos específicos externos o guías internas sobre las mejores prácticas. El MSS-EPS puede vigilar las desviaciones de estas líneas base y también puede “forzar” el cumplimiento de estas.

Los servicios que nos proporcionan información para esta sección no han sido contratados.

VALIDACIÓN DE CIBERSEGURIDAD

La validación de seguridad conlleva validar la totalidad de la seguridad a través de pruebas con ataques simulados. Estas pruebas se realizan con el Servicio Managed Breach Attack Simulation (MSS-BAS). El MSS-BAS es una colección avanzada de servicios de prueba que abarca pruebas pre-explotación, post-explotación y de percepción. Las pruebas se realizan sobre objetivos reales, utilizando ataques simulados, por lo tanto, proveen resultados concluyentes (sin falsos positivos). Los diferentes vectores de ataques prueban las de las contramedidas de la organización en diferentes factores como: configuraciones, implementaciones y habilidad de responder en forma continua produciendo recomendaciones e inteligencia valiosas

CONFIDENCIAL



a la organización.

Los servicios que nos proporcionan información para esta sección no han sido contratados.

ACCESO CONFIABLE

El nuevo modelo de TI viene con una superficie de ataque mayor, conformada por los empleados que utilizan sus dispositivos personales para el trabajo, mientras laboran de forma remota. La proliferación de aplicaciones en la nube para casi cualquier necesidad de negocio también ha contribuido al incremento de complejidad técnica. Hoy día, los atacantes pueden exponer diferentes vulnerabilidades en múltiples vectores en un solo ataque. La seguridad tradicional está diseñada para lidiar con ataques aislados o separados, haciendo estas soluciones poco efectivas contra las amenazas modernas. Estas nuevas amenazas se centran en obtener acceso remoto a sus aplicaciones y datos, ya sea con credenciales robadas o explotando vulnerabilidades conocidas dirigidas a sus usuarios, sus dispositivos desactualizados, aplicaciones en la nube y software de acceso remoto.

El Managed Trusted Access Service (MSS-TAS) es un servicio de seguridad integral para (a) garantizar que el acceso de los usuarios sea de confianza (usuario válido) y (b) los dispositivos utilizados por el usuario para autenticar cumplan con los estándares de seguridad de la organización.

Los servicios que nos proporcionan información para esta sección no han sido contratados.

CONFIDENCIAL



Recomendaciones

GLESEC recomienda BANVIVIENDA abordar lo siguiente:

1. Tome medidas inmediatas sobre las recomendaciones detalladas en este informe.
2. Tómese un tiempo para revisar los incidentes notificados durante este período, además de los incluidos en este y en los informes anteriores, y avísenos si son parte de la función normal de sus sistemas.
3. La mayoría de las vulnerabilidades encontradas pueden reforzarse considerando las mejores prácticas para implementar SSL/TLS cuando no se permiten versiones anteriores. SSL se ha convertido en un protocolo obsoleto y tiene muchas vulnerabilidades bien documentadas, como POODLE. Preste especial atención a los siguientes hosts: 200.46.2227.230, 200.46.19.100, 200.137.89 y 200.90.137.87.
4. Es importante configurar certificados válidos, ya que existen métodos de ataque que involucran la falsificación de un servicio como un correo web y porque el servicio oficial no tiene un certificado válido, es posible que los clientes crean que el servicio de atacantes es el objetivo. Esto podría provocar el robo de credenciales, la filtración de datos, entre otros.
5. Le recomendamos encarecidamente que no permita ninguna conexión a través de telnet (no está abierto, siempre es mejor filtrarlo si no se utiliza) a cualquiera de sus sistemas, independientemente si las conexiones se establecen dentro de la red local o a través de Internet. Es uno de los puertos más atacados en torno al 59%.
6. Sí los hosts 200.46.227.227 y 200.46.19.98 están escuchando en el puerto 80, recomendamos utilizar el puerto 443, ya que, aunque se interrumpieron los intentos de conexión desde el exterior, hemos registrado muchos intentos de varias direcciones IP, como: 200.46.73.116, 10.100.201.49, 104.248.119.106 y 104.248.67.229.
7. Tenga en cuenta que la vulnerabilidad de tipo Internet Key Exchange (IKE) Aggressive Mode with Pre-Shared Key que se describe en la sección Vulnerabilidades por gravedad del informe técnico, se está presentando en los hosts 200.46.227.227 y 200.46.19.98 que son vulnerables por el puerto 500 y utilizan el protocolo UDP.



Sección de Inteligencia por módulo de servicio.

Sección de inteligencia para el Servicio de Seguridad 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.

El propósito de esta sección es resaltar la Inteligencia recopilada de este y otros servicios contratados, así como también de fuentes externas como “honeypots”, fuentes maliciosas conocidas, base de datos de vulnerabilidades, relaciones con los equipos de CERT y CSIRT que GLESEC posee, en conjunto con otras fuentes de amenazas.

Los siguientes gráficos son tableros generados por la plataforma TIP™ de GLESEC. Estos tableros son representativos de las métricas para este servicio.

Es importante establecer un programa de gestión de vulnerabilidades como parte de la estrategia de seguridad de la información debido a que poco después que las vulnerabilidades son descubiertas y reportadas por investigadores de seguridad o proveedores, los atacantes desarrollan código para explotar las vulnerabilidades y lanzan ataques con este código contra destinos de interés. Cualquier demora significativa en encontrar o reparar software con vulnerabilidades peligrosas provee amplias oportunidades para que ataques persistentes logren pasar las defensas, obteniendo control sobre las máquinas vulnerables y obteniendo acceso sobre la información sensible contenida en los mismo. Las organizaciones que no realizan escaneos en busca de vulnerabilidades y no corrigen las fallas descubiertas de forma proactiva enfrentan una mayor probabilidad de tener sus sistemas comprometidos

Muchas de las vulnerabilidades proveerán información CVE. El CVE (Common Vulnerabilities and Exposures) es una lista de riesgos de seguridad y vulnerabilidades patrocinados por el US-CERT y mantenido por la Corporación MITRE. La misión del CVE es proveer nombres estándares para todos los riesgos de seguridad conocidos públicamente, así como también definiciones estándares para términos de seguridad. El CVE puede ser buscado en línea en la dirección <http://nvd.nist.gov/>

Puntuación de Vulnerabilidad

CONFIDENCIAL



La puntuación de vulnerabilidad está determinada por su factor de riesgo; crítico, alto, medio o bajo, así como también su valor en el Common Vulnerability Scoring System (CVSS). La “puntuación base” representa el riesgo innato de alguna característica de cada vulnerabilidad. El CVSS es un sistema de puntuación de vulnerabilidades designado para proveer un método estandarizado y abierto para calificar las vulnerabilidades de TI. CVSS ayuda a las organizaciones priorizar y coordinar una respuesta conjunta para resolver estas vulnerabilidades, comunicando las propiedades base, temporales y circunstanciales de cada vulnerabilidad. Adicional a los valores números, el CVSS provee clasificaciones de Alto, Medio y Bajo, pero estos rangos cualitativos están relacionados a los valores numéricos CVSS.

Las vulnerabilidades están catalogadas de esta forma:

Riesgo bajo si tienen una puntuación CVSS base de 0.0 – 3.9.

Riesgo medio si tienen una puntuación CVSS base de 4.0 – 6.9.

Riesgo alto si tienen una puntuación CVSS base de 7.0 – 10.0.

Información de Vulnerabilidades

Gráfica: Distribución de riesgo.

Esta gráfica muestra la distribución de riesgo de las vulnerabilidades descubiertas en el periodo de este reporte.

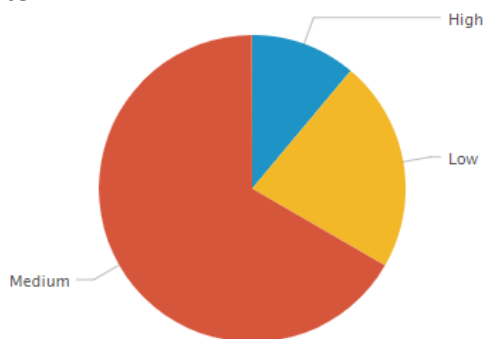


Gráfico: Categorías más frecuentes de vulnerabilidad.

Esta gráfica muestra la categoría de vulnerabilidad más frecuente descubiertas durante el periodo de este reporte.

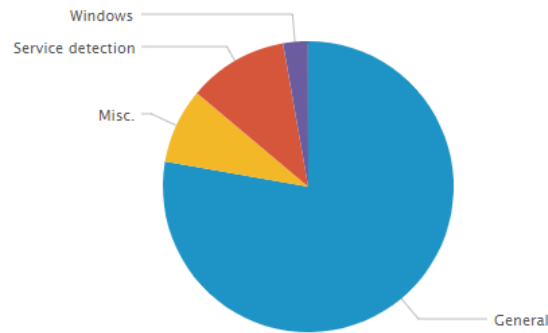


Gráfico: Nombre de vulnerabilidad más frecuente.

Esta gráfica muestra las vulnerabilidades más frecuentes descubiertas durante el periodo de este reporte.

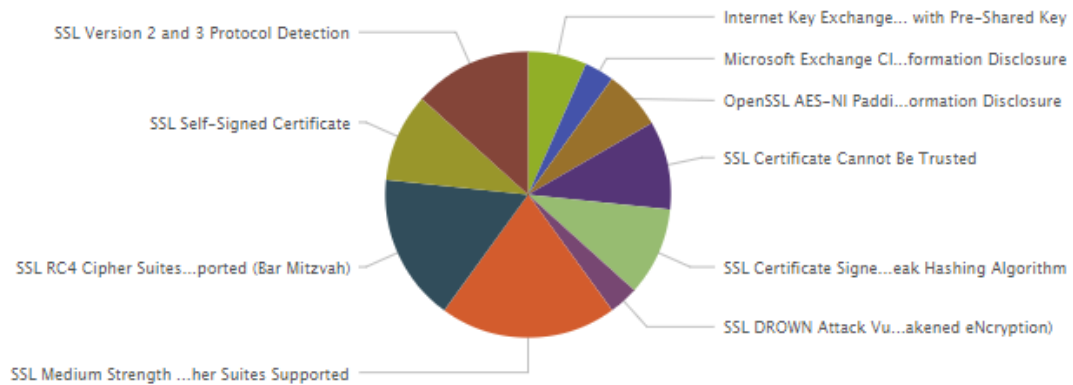


Gráfico: Hosts más vulnerables.

Este gráfico muestra los hosts más vulnerables descubiertos durante el periodo de este reporte.

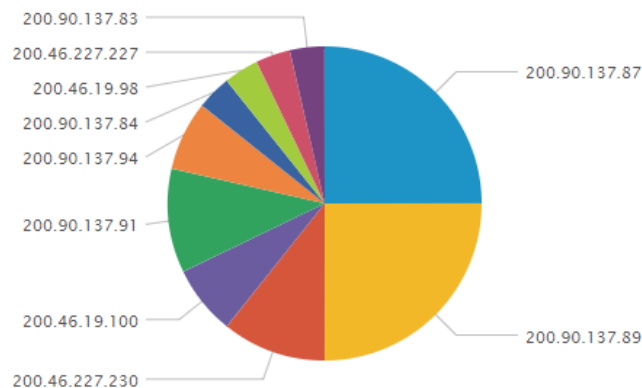


Gráfico: Riesgo de vulnerabilidad por nombre de vulnerabilidad.

Este gráfico ilustra el riesgo de las vulnerabilidades descubiertas y el conteo por nombre de vulnerabilidades durante el periodo de este reporte.

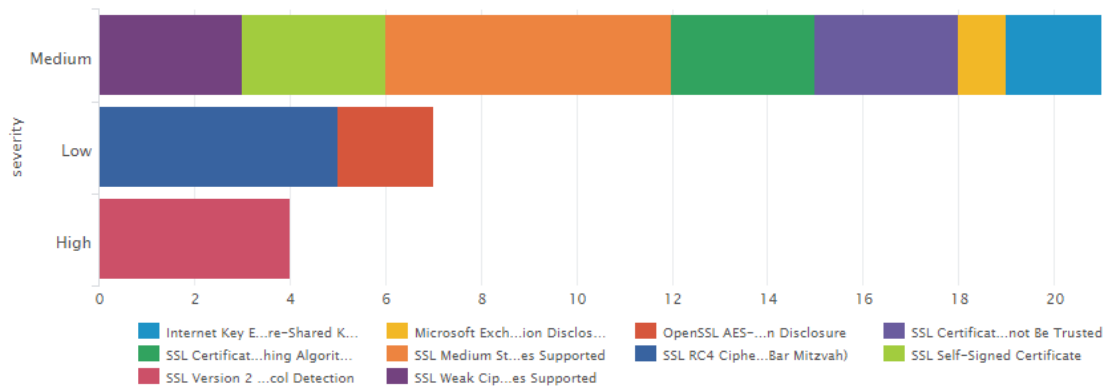


Gráfico: Riesgo de vulnerabilidad por host.

En el siguiente diagrama se puede identificar la proporción de ocurrencias de cada host con respecto al nivel de riesgo, encontradas durante este periodo.

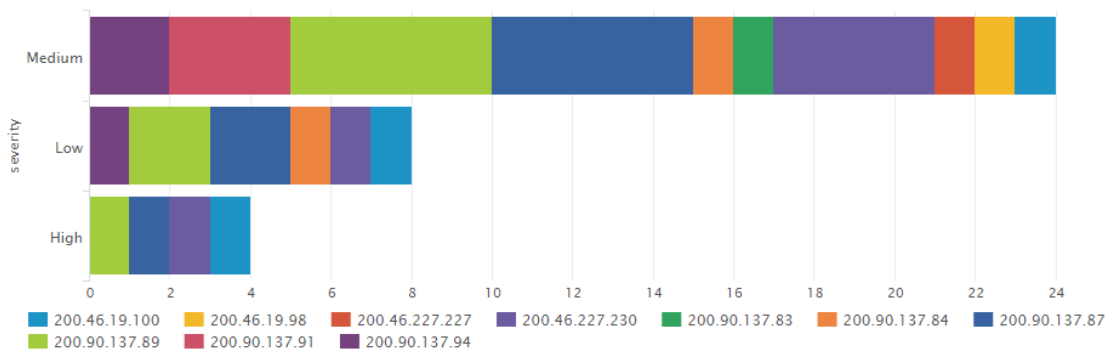


Gráfico: Riesgo de Vulnerabilidad por categoría.

Esta gráfica ilustra el riesgo de las vulnerabilidades descubiertas y su categoría durante el periodo de este reporte.

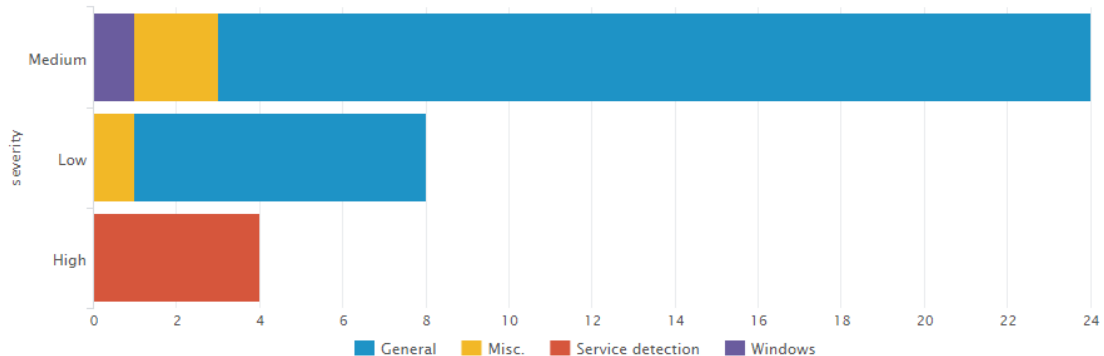


Gráfico: Riesgo de vulnerabilidad por puerto.

Esta gráfica ilustra el riesgo de las vulnerabilidades descubiertas y el conteo por puerto en el periodo de este reporte.

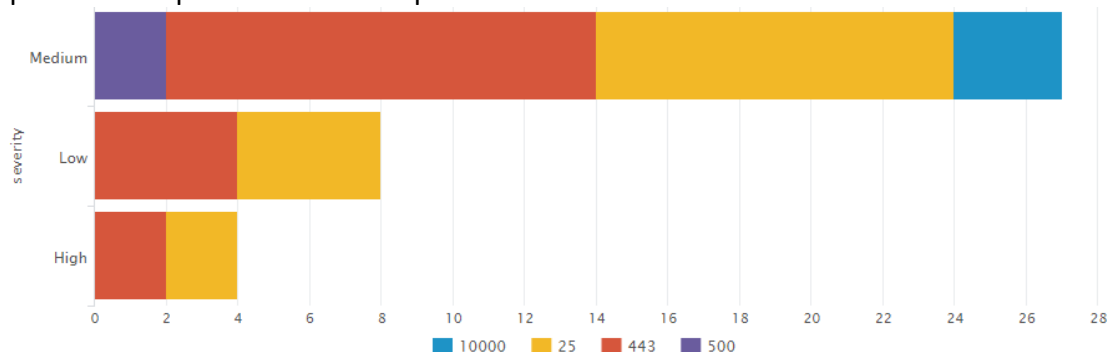


Gráfico: Riesgo de vulnerabilidad por protocolo.

Esta gráfica ilustra el riesgo de las vulnerabilidades descubiertas y el conteo por protocolo durante el periodo de este reporte.

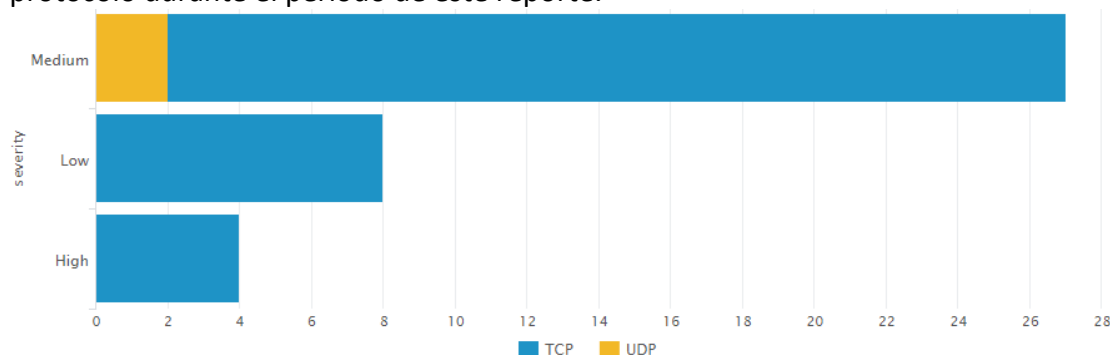


Gráfico: Categoría de vulnerabilidades por nombre de vulnerabilidad.

Este gráfico ilustra las categorías de vulnerabilidad descubiertas y el conteo por nombre de vulnerabilidad durante este periodo de reporte.

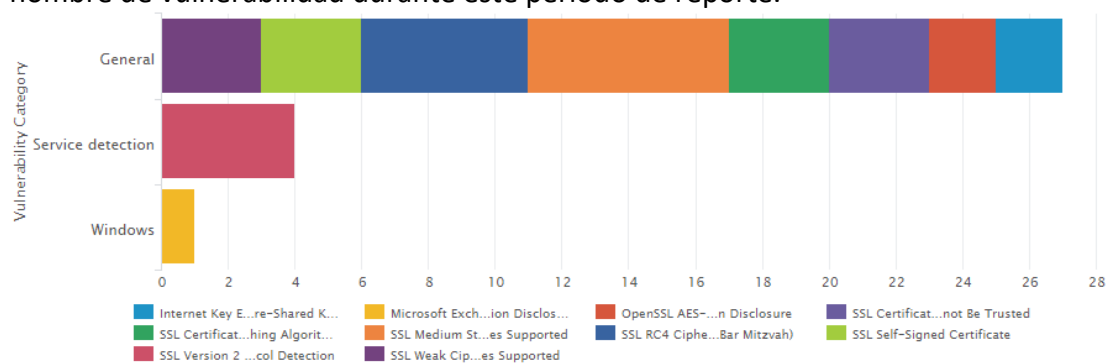


Gráfico: Categoría de vulnerabilidad por host.

Este gráfico ilustra las categorías de vulnerabilidad descubiertas y el conteo por hosts durante este periodo de reporte.

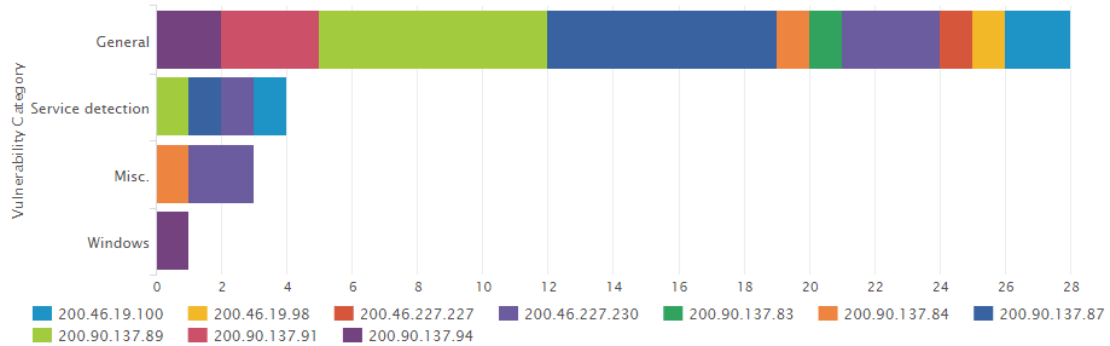


Gráfico: Categoría de vulnerabilidad por riesgo.

Este gráfico ilustra las categorías de vulnerabilidades descubiertas y el conteo por riesgo durante este periodo de reporte.

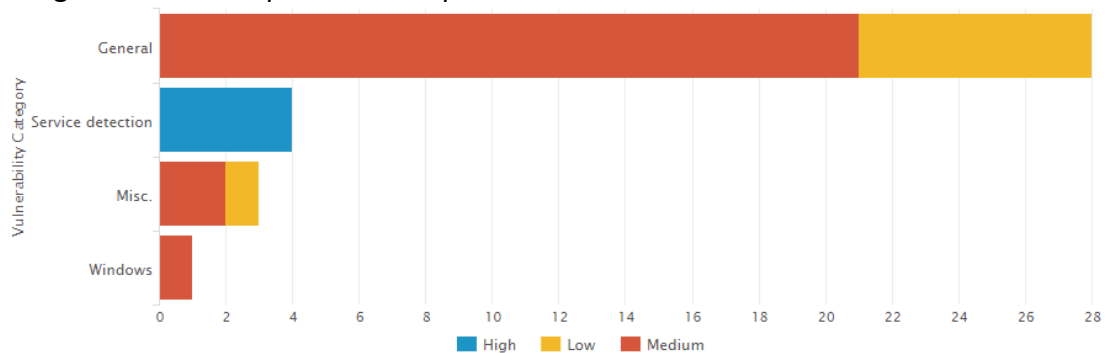


Gráfico: Categoría de vulnerabilidad por puerto.

Este gráfico ilustra las categorías de vulnerabilidades descubiertas y el conteo por puerto durante este periodo de reporte.

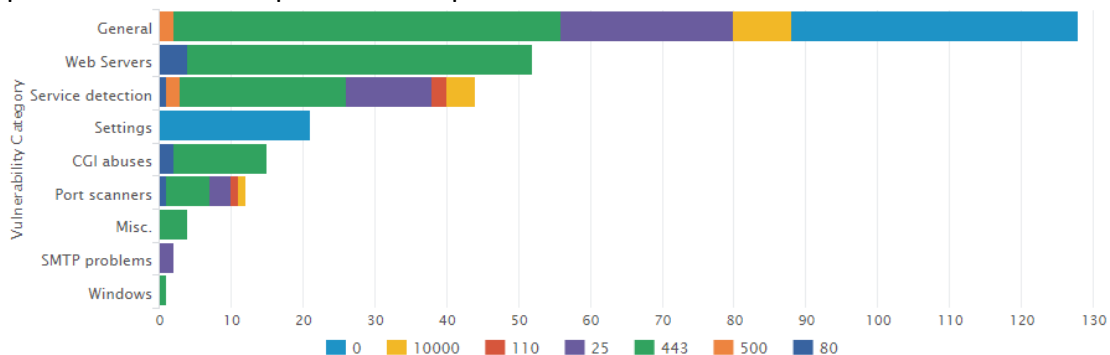


Gráfico: Categoría de vulnerabilidad por protocolo.

Este gráfico ilustra las categorías de vulnerabilidades descubiertas y el conteo por protocolo durante el periodo de este reporte.

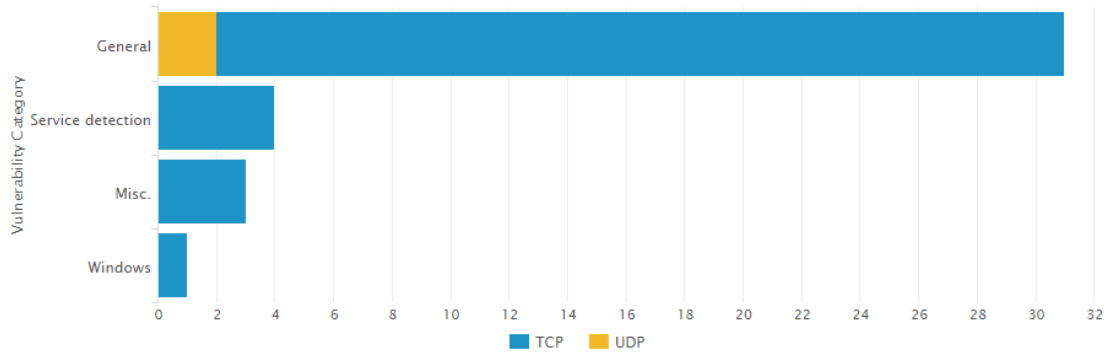


Gráfico: Nombre de vulnerabilidad por host.

Este gráfico ilustra las vulnerabilidades descubiertas y el conteo por hosts durante el periodo de este reporte.

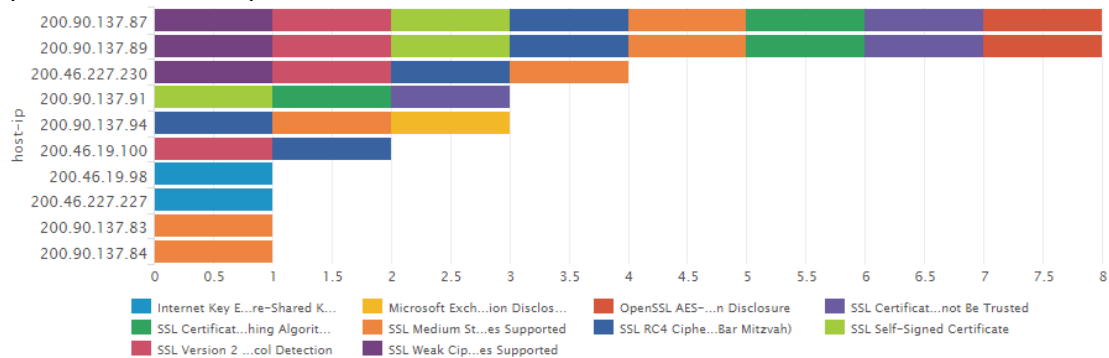


Gráfico Categoría de vulnerabilidad por host.

Este gráfico ilustra las categorías de las vulnerabilidades descubiertas y el conteo por hosts durante el periodo de este reporte.

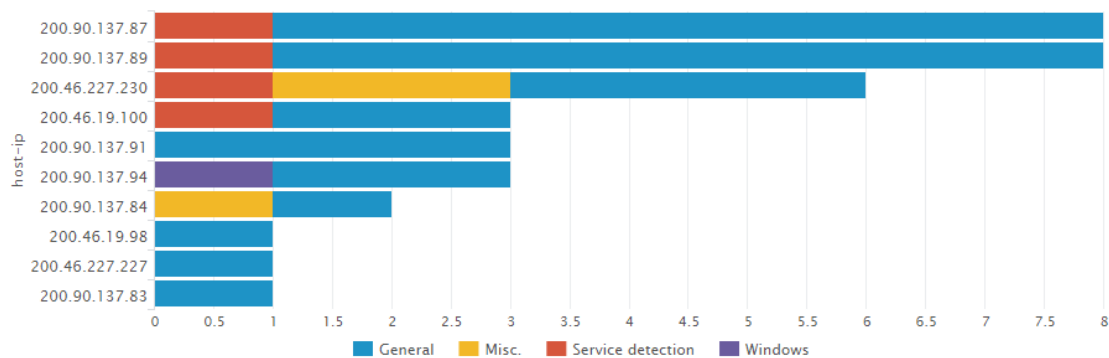


Gráfico: Riesgo de vulnerabilidad por host.

Esta gráfica ilustra el riesgo de las vulnerabilidades descubiertas y el conteo por hosts durante el periodo de este reporte.

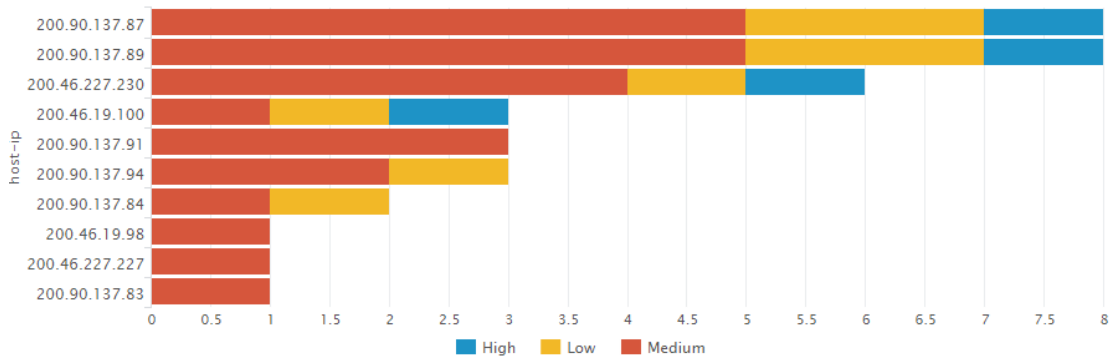


Gráfico: Puerto de vulnerabilidad por host.

Este gráfico ilustra el puerto de vulnerabilidad y el conteo por hosts durante el periodo de este reporte.

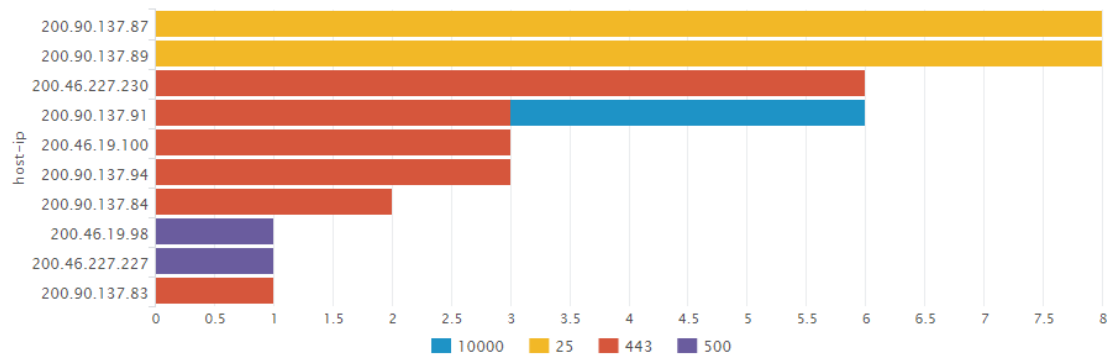
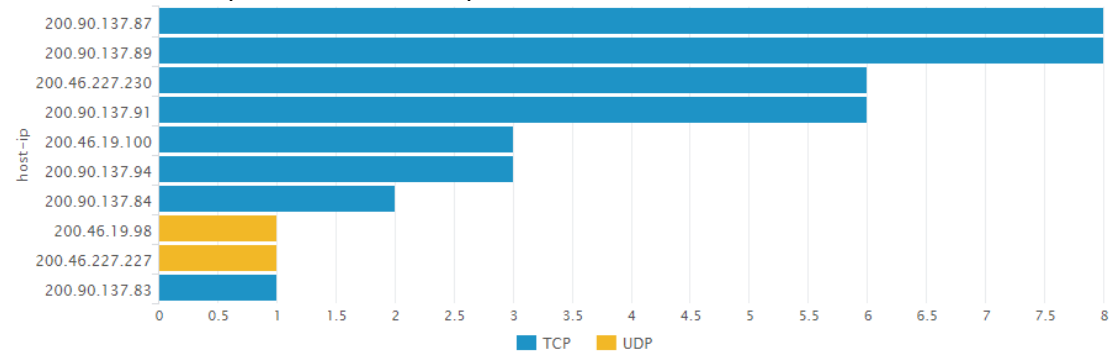


Gráfico: Protocolo de vulnerabilidad por host.

Este gráfico ilustra el protocolo de las vulnerabilidades descubiertas y el conteo por hosts durante el periodo de este reporte.



Sección de Inteligencia del 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.

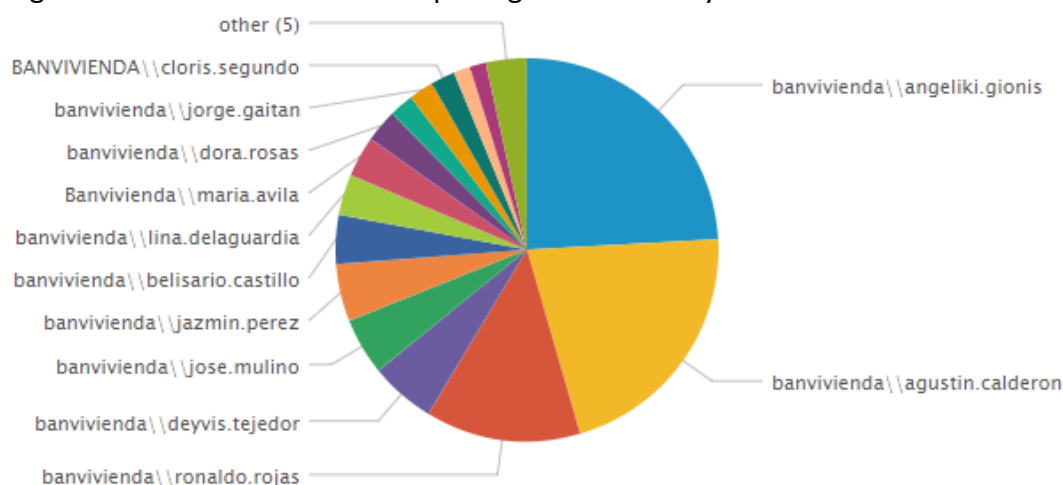
El propósito de esta sección es resaltar la inteligencia recolectada por este y otros servicios contratados, así como también fuentes externas como Honeypots, fuentes maliciosas conocidas, bases de datos vulnerables, relaciones con los equipos CERT y CSIRT que posee GLESEC, junto con otras fuentes de amenazas.

Los siguientes diagramas son tableros generados por la plataforma TIP™ de GLESEC. Estos tableros son representativos de métricas para este servicio.

Para este periodo BANVIVIENDA registro un total de 142 eventos relacionados a fuerza bruta, estos representan una severidad alta.

Gráfico: Principales Usuarios

Este gráfico muestra a los usuarios que registraron el mayor número de eventos.



Top eventos registrados

Durante este mes, nuestro GOC, recibió alertas generadas por las actividades de BANVIVIENDA, principalmente en el host:

- BpvExch02

Entre las alertas más frecuentes de este mes podemos citar:

- Intentos de fuerza bruta

En la siguiente tabla se muestra el total de eventos que registro cada usuario referente a este incidente.

Usuario	Cantidad
angeliki.gionis	35
agustin.calderon	31
rolando.rojas	19
deyvis.tejedor	8
jose.mulino	7
jazmin.perez	7
belisario.castillo	6
lina.delaguardia	5
maria.avila	5
dora.rosas	4
vielka.garcia	3
jorge.gaitan	3
cloris.segundo	3
joaquin.victoria	2
jezer.mock	2
rolando.rojas	1
jannet.giraldez	1

Todas estas alertas fueron revisadas y reportadas al cliente. Puede ver más detalles de estas alertas en nuestro informe técnico mensual.

CONFIDENCIAL

Sección de Inteligencia para el Servicio de Seguridad Administrado de Correlación de Eventos (MSS-SIEM)

El MSS-SIEM es una solución de correlación de eventos basado en el dispositivo de seguridad múltiple de GLESEC (GMSA) el cual cuando se conecta a la red interna de la organización permite la recepción de la data a ser correlacionada y genera inteligencia, alertas y reportes tanto como administración y manejo de incidentes.

El propósito de esta sección es resaltar la inteligencia recolectada por este y otros servicios contratados, así como también fuentes externas como Honeypots, fuentes maliciosas conocidas, bases de datos vulnerables, relaciones con los equipos CERT y CSIRT que posee GLESEC, junto con otras fuentes de amenazas.

Los siguientes diagramas son tableros generados por la plataforma TIPTM de GLESEC. Estos tableros son representativos de métricas para este servicio.

Gráfico: Conexiones denegadas

Este gráfico muestra las conexiones denegadas en las reglas del firewall.

341,008

Gráfico: Principales países bloqueados

Este gráfico muestra los principales países atacantes bloqueados.

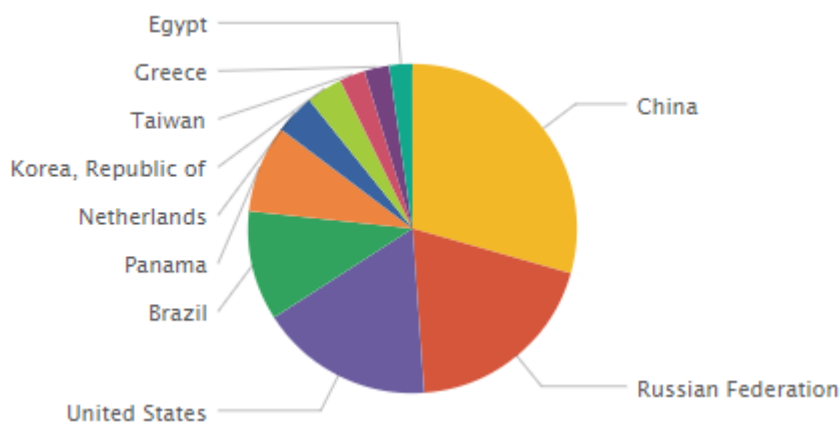


Gráfico: Fuentes principales

Este gráfico muestra las principales fuentes de ataque bloqueadas.

CONFIDENCIAL

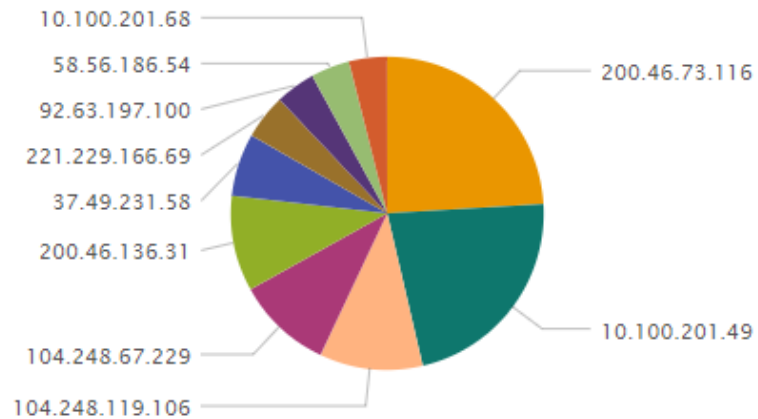


Gráfico: Ataques principales bloqueados por fuente

Este gráfico muestra las categorías de ataques por fuentes de ataque.

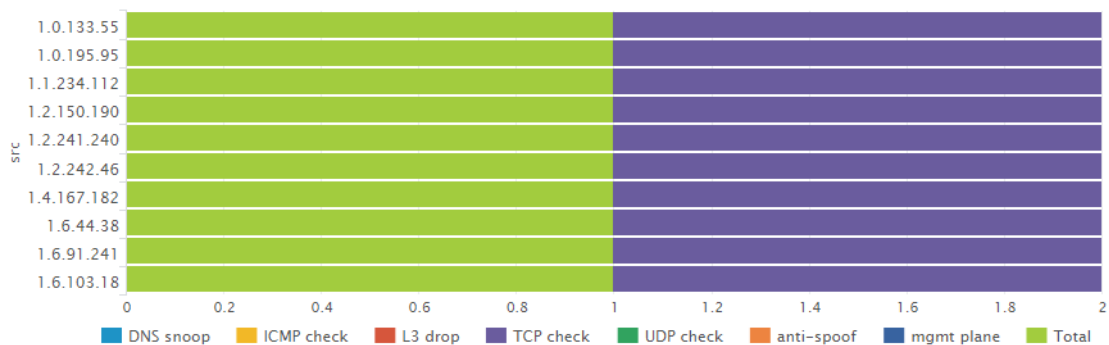


Gráfico: Tipos de ataques

Este gráfico muestra las principales categorías de ataques.

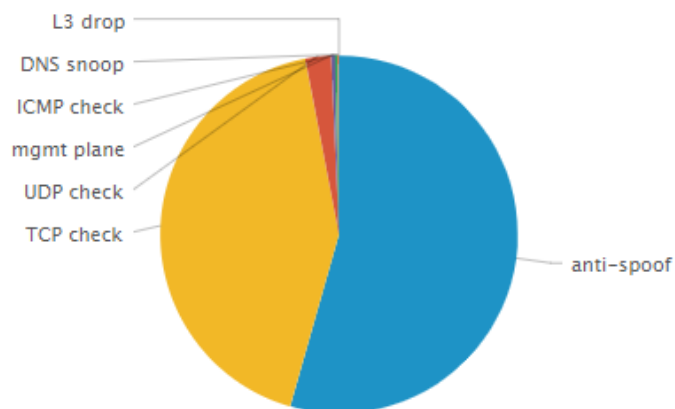


Gráfico: Puertos Atacados

Este gráfico muestra los principales puertos atacados.

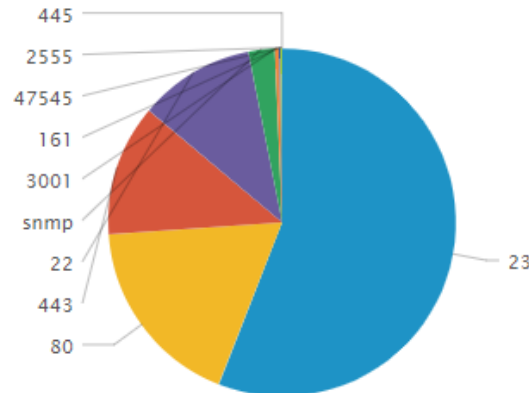


Gráfico: Destinos principales

Este gráfico muestra los principales destinos de ataque denegados.

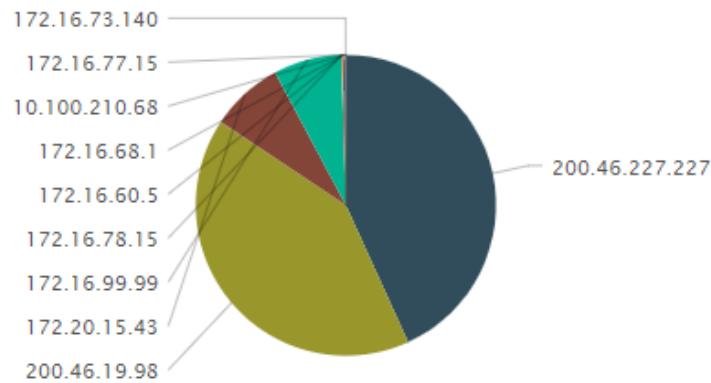


Gráfico: Servicios Principales

Este gráfico proporciona los servicios principales bloqueados por las reglas de firewall de entrada y salida.

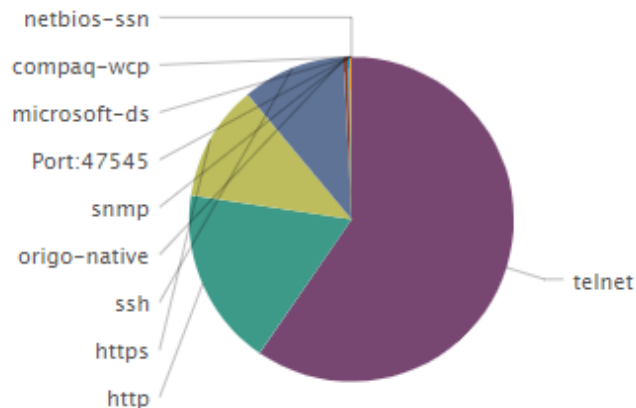


Gráfico: Amenazas principales

Este gráfico muestra la categoría de amenaza superior denegada.

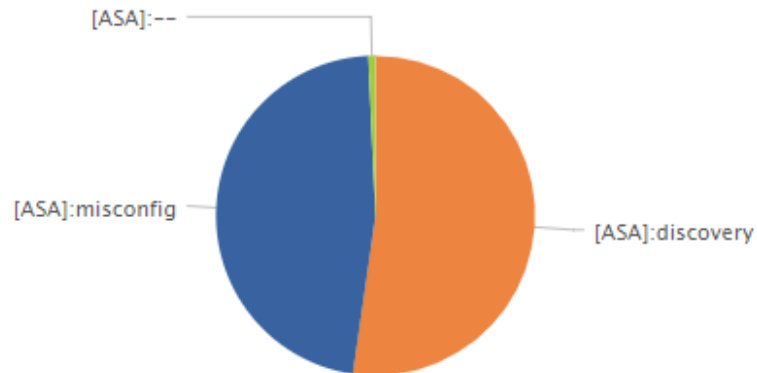


Gráfico: Acciones tomadas

Este gráfico muestra las acciones más frecuentes tomadas para negar ataques.

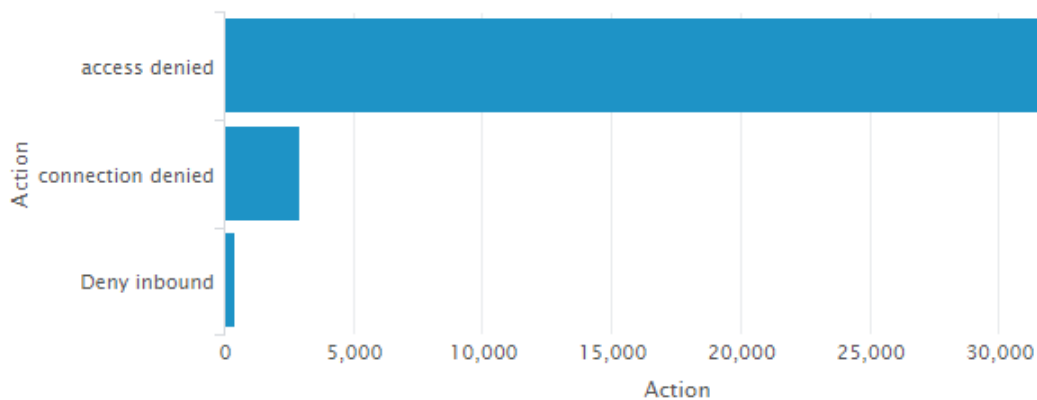


Gráfico: Actividad de red

Este gráfico muestra las categorías de tráfico más frecuentes presentes en la red.

vendor_definition	count	percent
Network Access Point	1022289	74.520908
IKE and IPsec	1022289	74.520908
User Session	343970	25.074081
Access Lists	309350	22.550417
IP Stack	5309	0.387006
NAT and PAT	2962	0.215918
High Availability (Failover)	246	0.017932
Command Interface	1	0.000073

CONFIDENCIAL

Operaciones de Ciber Seguridad

El propósito de esta sección es resaltar las actividades realizadas por el Centro de Operaciones Globales (GOC) de GLESEC, que incluyen: monitorear la disponibilidad y el rendimiento de los servicios bajo contrato, la gestión de cambios, las actividades de respuesta a incidentes y las actividades de consultoría.

ACTIVIDAD DE SERVICIOS PROFESIONALES

A continuación, describimos el uso del servicio de consultoría de la actividad de servicios profesionales para el mes correspondiente. En esta table mostramos el total de horas facturables y no facturables, el retenedor contratado, el total de horas utilizadas en el mes y las horas por encima del retenedor.

Billable consulting hours	Non-billable consulting hours	Contracted retainer hours	Total Hours utilized	Hours above retainer
0	0	1	0	0

ACTIVIDAD DE TICKETS

En esta sección reportamos todos los procesos de gestión de cambios y tickets de incidentes para este mes.

Monthly Reports Banvivienda 2018-10-01[..]

printed by De

Ticket#	Title	Created
2018103110000022	Notificación de ataques de fuerza bruta (Banvivienda 010)	2018-10-31 22:37:42
2018101110000828	Notificación de ataques de fuerza bruta (Banvivienda 007)	2018-10-11 22:19:46
2018100810000138	Notificación de fuerza bruta (Banvivienda 006)	2018-10-08 16:42:54
2018100710000041	Reporte Mensual de Operaciones Septiembre 2018	2018-10-07 12:15:44

Todos los servicios operados normalmente durante el mes de Octubre.

CONFIDENCIAL



Definiciones

Las **vulnerabilidades altas** se definen como una de las siguientes categorías: puertas traseras, acceso completo de lectura / escritura a los archivos, ejecución remota de comandos, posibles caballos de Troya o divulgación de información crítica (por ejemplo, contraseñas).

Las **vulnerabilidades medias** describen vulnerabilidades que exponen datos confidenciales, navegación de directorios, divulgación de controles de seguridad, facilitan el uso no autorizado de servicios o denegación de servicio a un atacante.

Las **vulnerabilidades bajas** describen vulnerabilidades que permiten la recopilación de información preliminar o sensible para un atacante o plantean riesgos que no están completamente relacionados con la seguridad, pero que pueden usarse en ingeniería social o ataques similares.

Las vulnerabilidades de SMB / NetBIOS podrían permitir la ejecución remota de código en los sistemas afectados. Un atacante que explote con éxito estas vulnerabilidades podría instalar programas; ver, cambiar, o eliminar datos; o crear nuevas cuentas con derechos de usuario privilegiado. Las mejores prácticas de firewall y las configuraciones de firewall predeterminadas estándar pueden ayudar a proteger las redes de ataques que se originan fuera del perímetro de la empresa. Las mejores prácticas recomiendan que los sistemas que están conectados a Internet tengan un número reducido de puertos expuestos.

Las vulnerabilidades simples de red afectan a protocolos como NTP, ICMP y aplicaciones de red comunes como SharePoint, entre otras. Esto no pretende ser una lista completa.

La autenticación y el cifrado son dos tecnologías entrelazadas que ayudan a garantizar que sus datos permanezcan seguros. La autenticación es el proceso de asegurar que ambos extremos de la conexión sean, de hecho, "quienes" dicen que son. Esto se aplica no solo a la entidad que intenta acceder a un servicio (como un usuario final) sino también a la entidad que proporciona el servicio (como un servidor de archivos o un sitio web). El cifrado ayuda a asegurar que la información dentro de una sesión no se vea comprometida. Esto incluye no solo leer la información dentro de un flujo de datos, sino también modificarla.

Si bien la autenticación y el cifrado tienen sus propias responsabilidades para asegurar una sesión de comunicación, la máxima protección solo se puede lograr cuando se combinan los dos. Por esta razón, muchos protocolos de seguridad contienen especificaciones de autenticación y cifrado.

CONFIDENCIAL





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

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

Info@glesec.com
www.glesec.com