



# Informe de seguridad

## Usuario de Test

Servidor Cloud



Periodo: **13/MAY/2018 - 20/MAY/2018**

# ÍNDICE

<b>RESUMEN</b>	<b>2</b>
<b>Visión general</b>	<b>3</b>
Comparativa con otros usuarios	5
Servicios e IPs incluidos en este informe	6
<b>Tráfico</b>	<b>7</b>
Tráfico inbound y outbound	8
Tráfico inbound y outbound por países	8
Tráfico por IP de origen	9
Aspectos clave	10
<b>Aplicaciones</b>	<b>11</b>
Aplicaciones por relevancia	12
Aplicaciones por número de amenazas (TOP 5)	14
Aspectos clave	16
<b>Amenazas</b>	<b>17</b>
Amenazas bloqueadas	19
Aspectos clave	22
Amenazas registradas	23
Aspectos clave	25
<b>Autenticación</b>	<b>26</b>
Aspectos clave	31

<b>Datos clave</b>	<b>32</b>
Aspectos clave globales de toda la red	33
<b>Definiciones y contramedidas</b>	<b>34</b>
Vulnerabilidad por desbordamiento	35
Ataque por fuerza bruta	36
Ejecución de código	37
Filtrado de información	38
<b>DETALLE DE AMENAZAS</b>	<b>39</b>
<b>Resumen de amenazas</b>	<b>40</b>
<b>Amenazas por Host</b>	<b>42</b>
Host 81.25.000.00	43
<b>Contacta con un asesor</b>	<b>50</b>
¿Necesitas ayuda sobre el informe?	51

# RESUMEN

---

La primera parte de este informe lo constituye un resumen de los datos obtenidos por nuestro Next Generation Firewall, incluyendo las amenazas, los hosts más afectados y otros datos estadísticos que permiten a tu equipo TI tomar decisiones de forma eficaz.

# 1

## Visión general

A continuación se presenta una visión global de las amenazas detectadas y bloqueadas durante los últimos 7 días. Según los ajustes actuales de sensibilidad, se han bloqueado las amenazas de perfil MEDIUM, HIGH o CRITICAL.

Periodo: **13/MAY/2018 - 20/MAY/2018**



**88** amenazas detectadas



**86** amenazas bloqueadas



**66** intentos de acceso ilegítimo

## Comparativa con otros usuarios

Mostramos el estado de la infraestructura monitorizada por nuestro Next Generation Firewall en comparación con otros clientes para dar una referencia de su estado.

### Aplicaciones en la red

El número de aplicaciones de los hosts incluidos en este informe es un +1100% del resto de usuarios.



### Media de amenazas por host

La media de amenazas a los hosts incluidos en este informe es un -26% del resto de usuarios.



### Media de intentos de intrusión por host

La media de intentos de intrusión en los hosts incluidos en este informe es un -10% del resto de usuarios.



## Servicios e IPs incluidos en este informe

La tabla inferior contiene la lista de todos los hosts incluidos en este informe.

SERVICIO	IP	AMENAZAS	AUTENTICACIÓN	ARCHIVOS
Servidor Cloud	81.25.000.00	88	66	0



# 2 Tráfico

El resumen de tráfico presenta información relevante sobre los datos transferidos por cada IP o servicio, la variación desde el último informe así como también un ranking de los países, aplicaciones y protocolos más frecuentes.

## Tráfico inbound y outbound

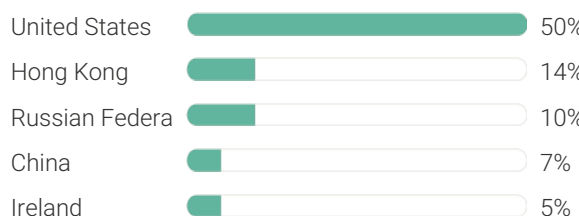
Se muestra el tráfico de datos de todos los hosts incluidos en este informe así como también la diferencia respecto al último informe. Recomendamos vigilar ante grandes variaciones.

SERVICIO	IP	INBOUND	IN DIFF.	OUTBOUND	OUT DIFF.
Servidor Cloud	81.25.000.00	12 MB	+97%	7 MB	+92%

## Tráfico inbound y outbound por países

La segmentación del tráfico por países permite detectar conexiones posiblemente ilícitas.

### INBOUND



### OUTBOUND



## Tráfico por IP de origen

Se muestran las principales direcciones IP con las que los hosts establecen conexiones entrantes y salientes.

### INBOUND



### OUTBOUND



## Aspectos clave

El apartado de tráfico permite detectar anomalías que podrían ser un indicio de actividad ilícita en los hosts. Cada empresa dispone de ciclos de actividad distintos que pueden variar de semana en semana. Por esta razón resulta importante comprobar si cualquier cambio en los resultados de este informe se corresponde con un cambio realizado en la compañía (una campaña, un evento interno, un lanzamiento de producto, etc).

- El host con mayor actividad esta semana ha sido Servidor Cloud.
- El país del que más tráfico se ha recibido ha sido United States (inbound) y Spain (outbound). ¿Son estos países esperados?
- Recomendamos revisar las direcciones IP listadas en este informe y asegurar que se correspondan con conexiones lícitas.

# 3 Aplicaciones

Nuestro Next Generation Firewall permite discriminar el tráfico según la aplicación que lo ha originado. Esta característica exclusiva de un firewall de capa 7 permite prevenir amenazas, aplicar soluciones específicas y detectar focos de riesgo con mucha más eficiencia.

## Aplicaciones por relevancia

La tabla inferior incluye una lista completa de todas las aplicaciones detectadas por nuestro Next Generation Firewall.

APLICACIÓN	SESIONES INBOUND	SESIONES OUTBOUND	AMENAZAS
smtp	7651	0	11
incomplete	931	0	0
mysql	894	0	55
web-browsing	699	24	14
insufficient-data	104	0	0
unknown-tcp	83	0	10
ssh	81	0	0
pop3	35	0	0
ftp	32	0	0
imap	20	0	0
t.120	12	0	0
ms-rdp	11	0	0

ssl	10	0	0
webdav	8	0	8
socks	7	0	0
http-proxy	4	0	0
irc-base	4	0	0
unknown-udp	3	0	0
ms-ds-smb-base	2	0	0
rsync	2	0	0
oracle	2	0	0
tacacs-plus	2	0	0
rmi-iiop	2	0	0
mssql-db	1	0	0

## Aplicaciones por número de amenazas (TOP 5)

Estas son las 5 aplicaciones que han recibido más amenazas (bloqueadas y no bloqueadas). En el apartado "Detalle de amenazas" de este informe encontrarás información detallada sobre la naturaleza, la prevención y las técnicas para mitigar todas estas amenazas.

### mysql

Se han detectado un total de 55 intentos de amenaza para esta aplicación.

AMENAZAS	CATEGORÍA	RIESGO	INTENTOS
MySQL Authentication Brute Force At	brute-force	HIGH	55

### web-browsing

Se han detectado un total de 14 intentos de amenaza para esta aplicación.

AMENAZAS	CATEGORÍA	RIESGO	INTENTOS
Apache Struts Jakarta Multipart Par	code-execution	CRITICAL	3
Oracle WebLogic WLS Security Compon	code-execution	HIGH	9
ZmEu Scanner Detection(34605)	info-leak	LOW	2

### smtp

Se han detectado un total de 11 intentos de amenaza para esta aplicación.

AMENAZAS	CATEGORÍA	RIESGO	INTENTOS
MAIL: User Login Brute Force Attemp	brute-force	HIGH	11



## webdav

Se han detectado un total de 8 intentos de amenaza para esta aplicación.

AMENAZAS	CATEGORÍA	RIESGO	INTENTOS
Microsoft IIS WebDAV ScStoragePathF	overflow	CRITICAL	8

## Aspectos clave

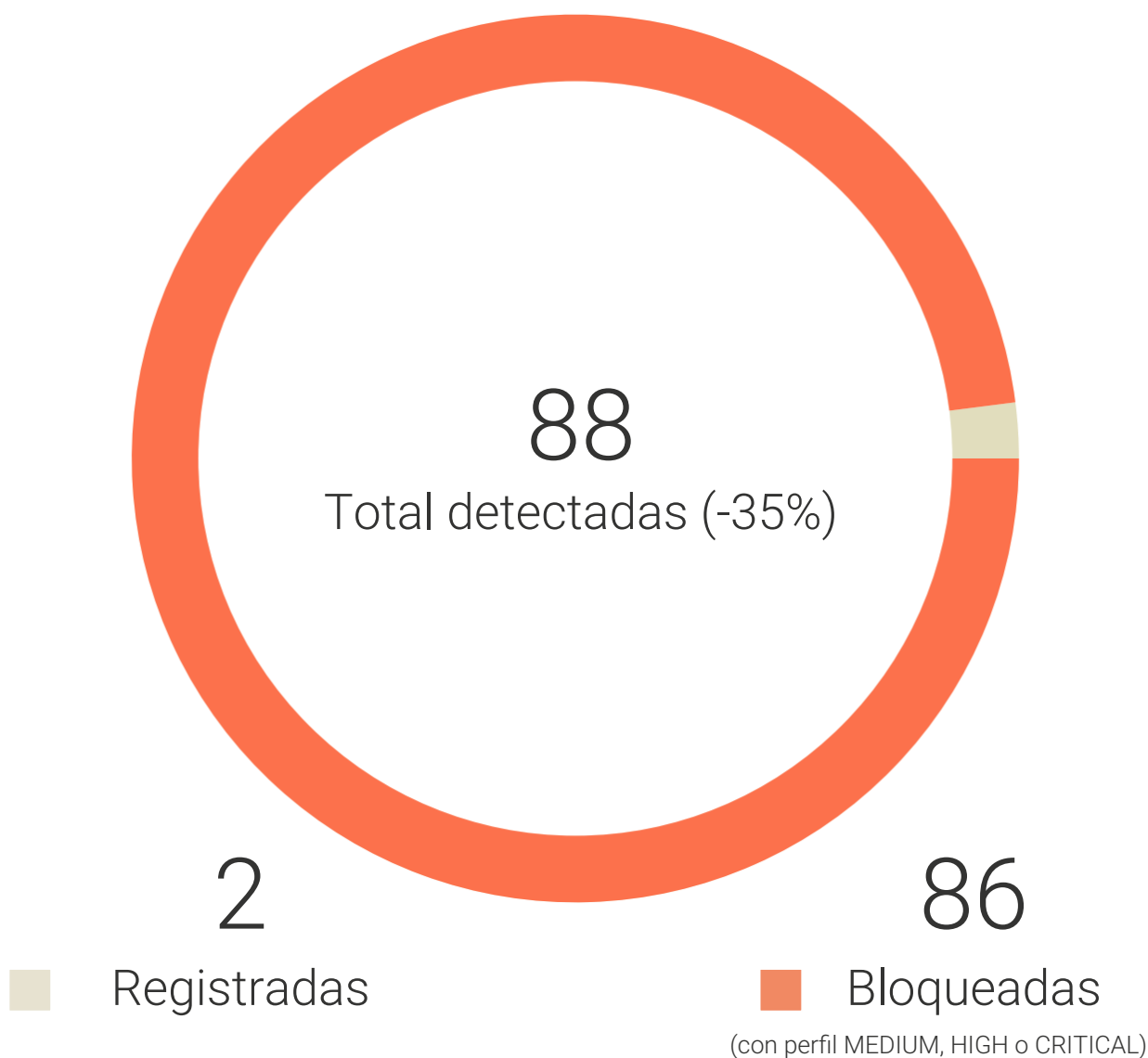
Una de las características clave de nuestro Next Generation Firewall es su capacidad para detectar qué aplicación origina o recibe cierto tipo de tráfico. Esta lista permite detectar actividad ilícita en los hosts o tener constancia de cuáles son las aplicaciones que suponen un mayor riesgo.

Es imprescindible contrastar las aplicaciones de esta lista con aquellas autorizadas y conocidas por la compañía.

- Los hosts incluidos en este informe han enviado o recibido tráfico mediante un total de 24 aplicaciones. La media de nuestros clientes es de 2 aplicaciones.
- La aplicación más común en los hosts incluidos en este informe es smtp (Inbound) y ntp (Outbound).
- Las cinco aplicaciones más comunes acumulan un total de 88 vulnerabilidades. Entre ellas, 11 son críticas. ¡Deben ser tomadas en consideración de inmediato!
- Las aplicaciones más vulnerables en sus hosts son: mysql, web-browsing, smtp, webdav
- Por favor, descarga el archivo CSV desde su panel de control para conocer en detalle todas las amenazas sucedidas para cada aplicación y host afectado.

# 4 Amenazas

A continuación se presenta un resumen y un listado de las amenazas detectadas por nuestro servicio de seguridad. En primer lugar se presentarán las amenazas que han sido bloqueadas en correspondencia con la sensibilidad elegida. Posteriormente, se presentan las amenazas que han sido registradas pero sobre las cuales nuestro sistema automático no ha tomado ninguna medida adicional.





## Amenazas bloqueadas

Nuestro NGFW ha bloqueado un total de 86 amenazas con perfil MEDIUM, HIGH o CRITICAL. Esta cifra representa una variación de -34% respecto al anterior informe.

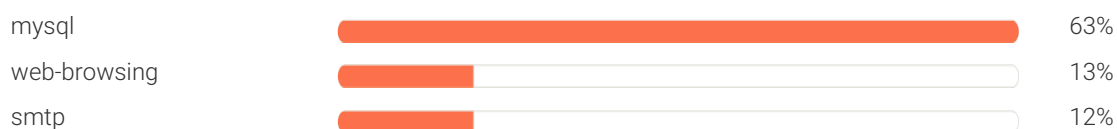
## Amenazas más relevantes (top 5)

Las amenazas mostradas a continuación han sido BLOQUEADAS en tiempo real. Esto significa que han sido detenidas y no han llegado a su destino.

AMENAZAS	CATEGORÍA	INTENTOS	CLASIFICACIÓN
Microsoft IIS WebDAV ScStoragePathFrom	overflow	8	CRITICAL
Apache Struts Jakarta Multipart Parser	code-execution	3	CRITICAL
MySQL Authentication Brute Force Attem	brute-force	55	HIGH
MAIL: User Login Brute Force Attempt(4	brute-force	11	HIGH
Oracle WebLogic WLS Security Component	code-execution	9	HIGH

## Aplicaciones más afectadas

Estas aplicaciones son las que actualmente suponen un mayor riesgo para su infraestructura al concentrar el mayor número de amenazas graves.





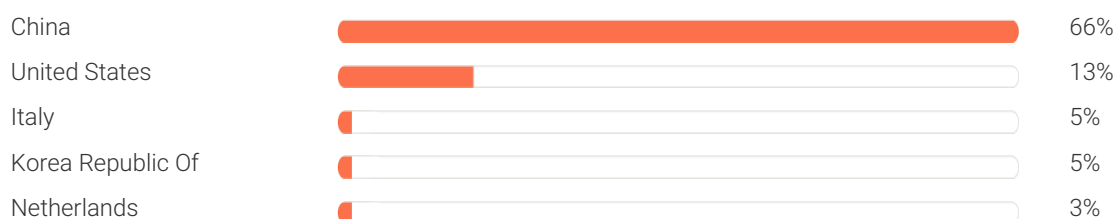
webdav



9%

## Origen de las amenazas

Conocer el origen de las amenazas puede ser útil a la hora de establecer mecanismos de prevención o reglas de filtrado para prevenir otras amenazas.



## Destino de las amenazas

La lista de destino de amenazas permite conocer cuáles son los hosts que concentran un mayor número de amenazas graves y que requieran una atención más inmediata para prevenir posibles factores de riesgo.



## Aspectos clave

Las amenazas son bloqueadas por nuestro Next Generation Firewall en tiempo real según la sensibilidad elegida en el panel de control. Todas las amenazas bloqueadas incluidas en este informe han sido interceptadas exitosamente y se ha impedido que todas ellas pudieran llegar al host destino.

Estas amenazas suponen una fuente de información esencial para detectar posibles vulnerabilidades y poder tomar medidas preventivas para proteger los hosts según el nivel de riesgo existente.

- Los perfiles de severidad bloqueados han sido: MEDIUM, HIGH o CRITICAL (según configuración de usuario).
- Nuestro NGFW ha bloqueado una media de 88 intentos de amenaza por host. La media de nuestros clientes es de 119 intentos de amenazas por host.
- El número de amenazas bloqueadas esta semana ha variado un -34% respecto al informe anterior.
- Las aplicaciones más afectadas son mysql, web-browsing, smtp, webdav. Por favor revisa la configuración de seguridad de estas aplicaciones en los hosts afectados.
- Los tipos de amenaza más comunes han sido overflow, code-execution, brute-force.
- El origen más común de las amenazas bloqueadas ha sido China.





### Amenazas registradas

Nuestro NGFW ha registrado, pero no bloqueado, un total de 2 amenazas con perfil LOW.

### Amenazas más relevantes (top 5)

Las amenazas mostradas a continuación han sido registradas por nuestro Next Generation Firewall pero no detenidas debido a que no cuentan con una severidad suficientemente alta según la actual configuración de usuario.

AMENAZAS	CATEGORÍA	INTENTOS	CLASIFICACIÓN
ZmEu Scanner Detection(34605)	info-leak	2	LOW

### Aplicaciones más afectadas

Estas aplicaciones concentran el mayor número de amenazas que han sido detectadas.

web-browsing



100%

## Origen de las amenazas

Conocer el origen de las amenazas puede ser útil a la hora de establecer mecanismos de prevención o reglas de filtrado para prevenir otras amenazas.



## Destino de las amenazas

La lista de destino de amenazas permite conocer qué hosts son los que concentran un mayor número de amenazas y que tienen que ser revisados para prevenir posibles factores de riesgo.



## Aspectos clave

Las amenazas registradas por nuestro Next Generation Firewall suponen una fuente de información vital para conocer el estado de seguridad de nuestra infraestructura y, de esta forma, poder preparar medidas de seguridad preventiva que contribuyan a proteger los hosts.

Estas amenazas NO han sido bloqueadas puesto que su nivel de severidad no era suficientemente alto y, por lo tanto, no suponían una amenaza inmediata. Recordamos que la sensibilidad del módulo de bloqueo en tiempo real puede ser ajustada desde el panel de control.

- Los perfiles de severidad registrados han sido: LOW (según configuración de usuario).
- Nuestro NGFW ha detectado una media de 88 intentos de amenaza por host. La media de nuestros clientes es de 119 intentos de amenazas por host.
- El número de amenazas detectadas esta semana ha aumentado un -35% respecto al informe anterior.
- Las aplicaciones más afectadas han sido web-browsing.
- Los tipos de amenaza más comunes han sido info-leak.
- El origen más común de las amenazas detectadas ha sido Germany.

# 5

# Autenticación

Este resumen i el consiguiente log listan intentos de acceso de fuerza bruta a los hosts monitorizados. Esta información podria ofrecer indicaciones sobre dónde es más necesario incrementar o revisar las actuales medidas de seguridad.

### Intentos de autenticación más relevantes (top 5)

La tabla que se muestra a continuación presenta un resumen de los principales intentos de intrusión en los hosts por fuerza bruta. A pesar de la gravedad aparente cabe destacar que muchos de estos ataques se realiza de forma automatizada a cualquier sistema conectado a internet, razón por la cual no suponen un riesgo verdadero si el sistema operativo ha sido actualizado, las aplicaciones disponen de una correcta configuración y las contraseñas son suficientemente seguras.

PROTOCOLO	SERVICIOS	IP	INTENTOS
MySQL Authentication Brute Force At	Servidor Cloud	81.25.000.00	55
MAIL: User Login Brute Force Attemp	Servidor Cloud	81.25.000.00	11

## IPs de origen más detectadas

Las IPs listadas a continuación acumulan un mayor número de intentos de intrusión a los hosts incluidos en este informe.



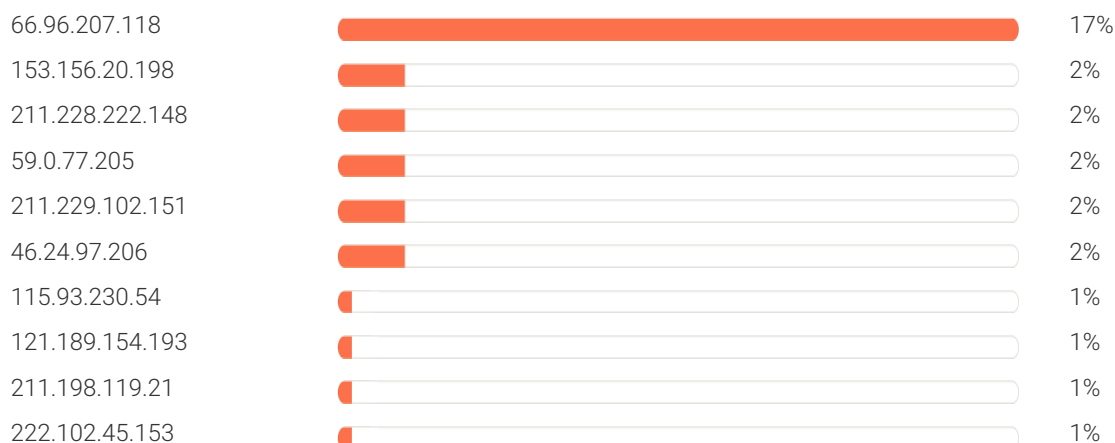
## Destino de las amenazas

La siguiente lista muestra los hosts afectados por intentos de autenticación ilegítima, ordenados por el número de intentos recibidos durante el período que comprende este informe.















## IPs origen de sesiones establecidas

Estas son las direcciones IP desde las que se ha establecido una conexión SSH con sus hosts y se ha mostrado a solicitante, al menos, la pantalla de login (no implica un login exitoso). ¿Son conocidas todas estas direcciones?



47.59.206.193		1%
59.1.53.25		1%
76.251.106.178		1%
93.170.95.65		1%
118.40.179.35		1%
125.132.212.243		1%
211.224.26.241		1%
222.105.8.176		1%
59.0.77.1		1%
59.1.64.242		1%
78.108.108.19		1%
106.240.97.82		1%
118.45.126.250		1%
222.114.50.37		1%
59.27.13.254		1%
78.235.137.30		1%
109.255.218.82		1%
119.205.97.143		1%
175.196.182.33		1%
222.99.219.134		1%
59.0.77.246		1%
59.28.189.48		1%
80.86.100.164		1%
112.162.190.169		1%
121.157.145.4		1%
175.199.11.155		1%
218.156.188.40		1%
223.171.34.99		1%
59.0.77.3		1%
59.30.245.231		1%
83.228.69.74		1%
112.218.21.227		1%
121.171.156.192		1%
175.206.108.143		1%
220.116.155.243		1%
24.202.29.217		1%
59.0.77.40		1%

61.40.102.134		1%
85.203.78.181		1%
112.220.146.213		1%
121.183.116.21		1%
175.212.45.162		1%
220.81.189.106		1%
37.11.96.95		1%
59.0.77.45		1%
61.40.167.218		1%
86.31.186.146		1%
115.90.155.22		1%
121.187.155.187		1%
175.215.131.136		1%
221.162.25.233		1%
59.1.133.199		1%
88.187.235.127		1%



## Aspectos clave

El apartado de autenticación lista las amenazas de acceso por fuerza bruta que pueden comprometer tus hosts. Recomendamos prestar especial atención a estas amenazas e implementar de inmediato medidas preventivas como, por ejemplo, sistemas automáticos de detección y bloqueo de IPs. Asimismo, recomendamos revisar la configuración de todas las aplicaciones y protocolos afectados.

Recordamos que todas las amenazas listadas en este apartado son consideradas de severidad CRITICAL y que han sido bloqueadas en tiempo real según la configuración del usuario.

- Se ha detectado una media de 66 intentos de autenticación/intrusión por host. La media de nuestros clientes es de 74 intentos por host.
- Recomendamos bloquear las IPs de origen de dichos intentos de autenticación e intrusión.

# 6

## Datos clave

De acuerdo con los datos presentados en este informe, presentamos un listado no exhaustivo de los aspectos más importantes que creemos se deberían tener en cuenta.

### **Aspectos clave globales de toda la red**

- El total del tráfico en su red ha crecido por sobre de un 50% respecto al último informe. Usted debería contactar de inmediato con el departamento de sistemas para evitar fallos en su servicio.
- El total del tráfico saliente de su red ha crecido por sobre de un 50% respecto al último informe. Esto es un claro indicador de que un ataque informático está siendo lanzado desde sus sistemas.
- Hemos detectado que un gran número de amenazas detectadas en sus sistemas se concentran en un solo tipo de aplicación. Usted debería revisar el uso de dicha aplicación así como su estado de seguridad y actualizaciones.
- Hemos detectado que el total de sus amenazas ha crecido respecto al global. Dependiendo de la envergadura de sus sistemas, esto puede ser algo relativamente normal. Sin embargo le recomendamos contactar con nosotros lo antes posible para estudiar esta situación.

Este listado ha estado generado de forma automatizada y no es exhaustivo. Por favor considera hablar con uno de nuestros asesores en ciberseguridad para obtener más datos clave y consejos sobre como protegerte de las amenazas detectadas.

# 7

## Definiciones y contramedidas

Presentamos a continuación información, consejos y datos clave sobre las amenazas más relevantes recogidas en este informe. El propósito de esta información es proveer a tu equipo TI consejos útiles que puedan ser implementados de forma inmediata, especialmente para aquellas amenazas de carácter crítico.

## Vulnerabilidad por desbordamiento (+100%)

Un exploit de tipo "buffer overflow" ha sido detectado en el tráfico de su red. Este tipo de exploits pueden permitir a un atacante la ejecución de código en la máquina atacada.

Gravedad:

**CRITICAL**

Este período:

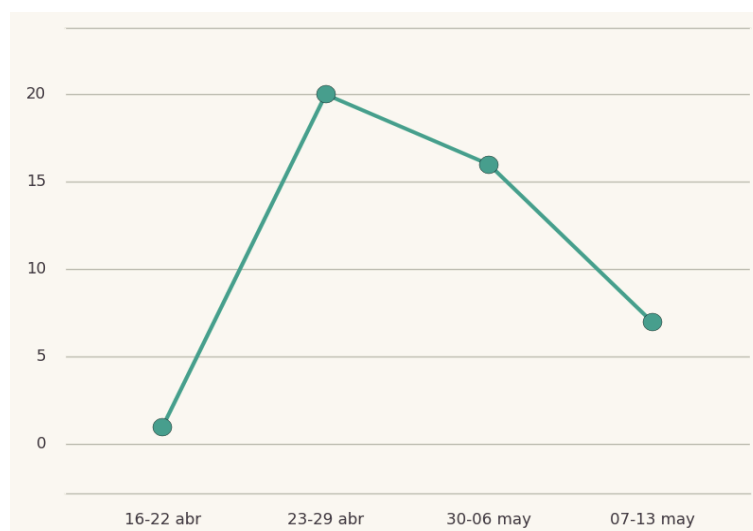
**8 (+100%)**

Host más afectado:

**Servidor Cloud**

Aplicaciones afectadas:

**webdav**



## Contramedida

Existen ciertos principios a considerar para proteger nuestras aplicaciones:

La mejor solución para evitar este tipo de vulnerabilidad consiste en mantener sus sistemas actualizados. Este tipo de vulnerabilidades suelen afectar en mayor medida a sistemas no actualizados.

## Ataque por fuerza bruta (-48%)

Un ataque por fuerza bruta consiste en un atacante intentando acceder a una máquina probando un gran número de usuarios y contraseñas a la vez. Este tipo de ataque es muy frecuente en internet actualmente.

Gravedad:

**HIGH**

Este período:

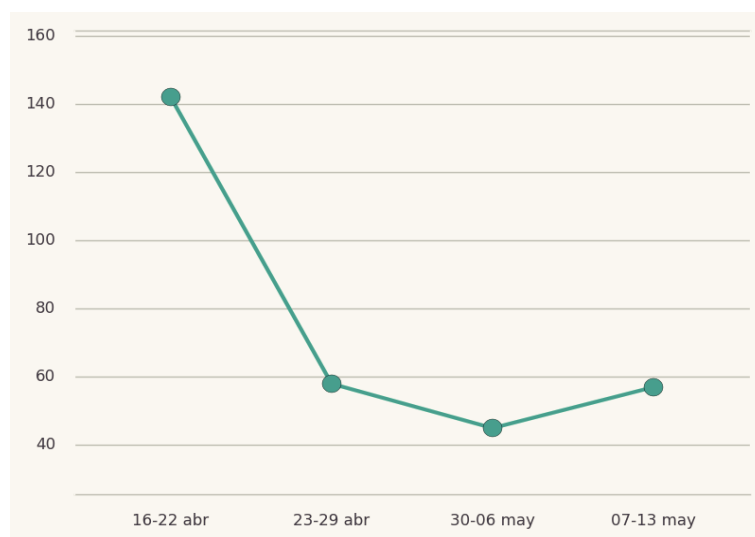
**66 (-48%)**

Host más afectado:

**Servidor Cloud**

Aplicaciones afectadas:

**mysql**



## Contramedida

Existen ciertos principios a considerar para proteger nuestras aplicaciones:

La mejor solución para afrontar este tipo de ataques consiste en establecer una buena política de seguridad en cuanto tanto al cortafuegos como al acceso por software a los sistemas.

## Ejecución de código (+1100%)

La ejecución de código es uno de los riesgos más peligrosos de la red. Un ataque mediante un exploit puede derivar en una amenaza por ejecución de código, un ataque mediante ransomware también entra en esta categoría. La ejecución de código malicioso puede comprometer todo un sistema informático.

Gravedad:

**HIGH**

Este período:

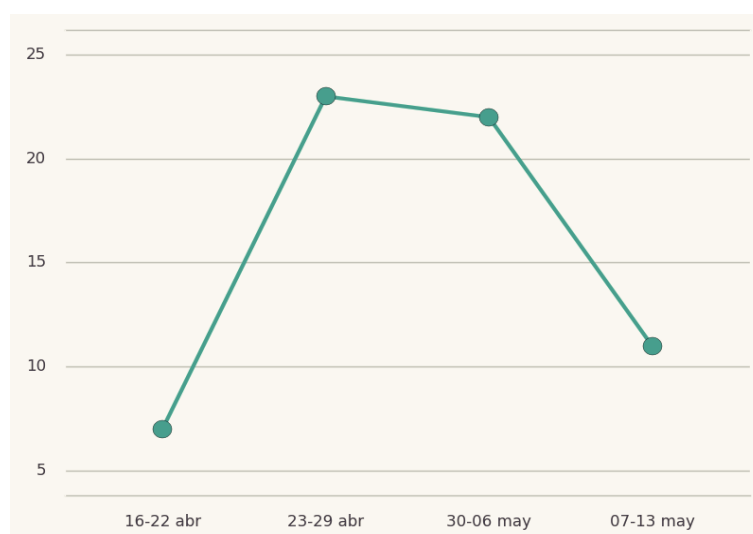
**12 (+1100%)**

Host más afectado:

**Servidor Cloud**

Aplicaciones afectadas:

**web-browsing**



## Contramedida

Existen ciertos principios a considerar para proteger nuestras aplicaciones:

La mejor manera de mitigar este tipo de ataques consiste en establecer una buena política de filtrado de amenazas a nivel de capa 7. Instalar software antivirus así como mantener los equipos actualizados es un requerimiento importante.

## Filtrado de información (-33%)

El filtrado de información es un problema común en muchas redes tanto internas como externas. La información considerada crítica es susceptible a ser filtrada y puede incluir:: cuentas bancarias, tarjetas de crédito, correos personales, direcciones físicas o números de teléfonos. Nuestros sistemas han detectado información personal dentro del tráfico de su red.

Gravedad:

**LOW**

Este período:

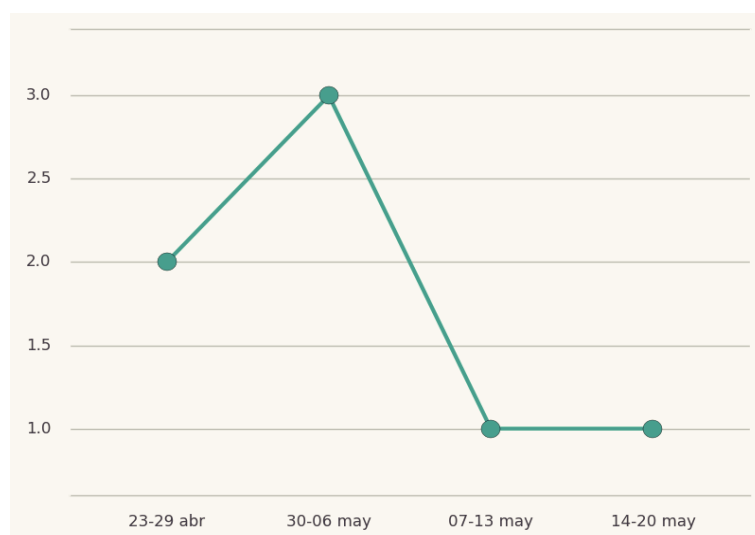
**2 (-33%)**

Host más afectado:

**Servidor Cloud**

Aplicaciones afectadas:

**web-browsing**



## Contramedida

Existen ciertos principios a considerar para proteger nuestras aplicaciones:

El administrador de la red debería tomar medidas para que la información sensible no pueda ser filtrada: buenas medidas pueden incluir el cifrado de archivos o la aplicación de grupos de usuarios con permisos determinados.



# DETALLE DE AMENAZAS

---

La segunda parte de este informe incluye información detallada sobre todas las amenazas detectadas por nuestro Next Generation Firewall así como también sobre la acción tomada. Las amenazas se encuentran clasificadas por host, ordenadas por gravedad e incluyen datos CVE actualizados hasta la fecha.

# 8 Resumen de amenazas

Debajo encontrará una vista general de la mayoría de amenazas detectadas en su red por nuestro Next Generation Firewall. Todas las amenazas han sido bloqueadas eficazmente y solo han sido registradas para ayudarte a encontrar una solución a largo plazo para posibles vulnerabilidades.

11

■ Critical

75

■ High



0

■ Medium

2

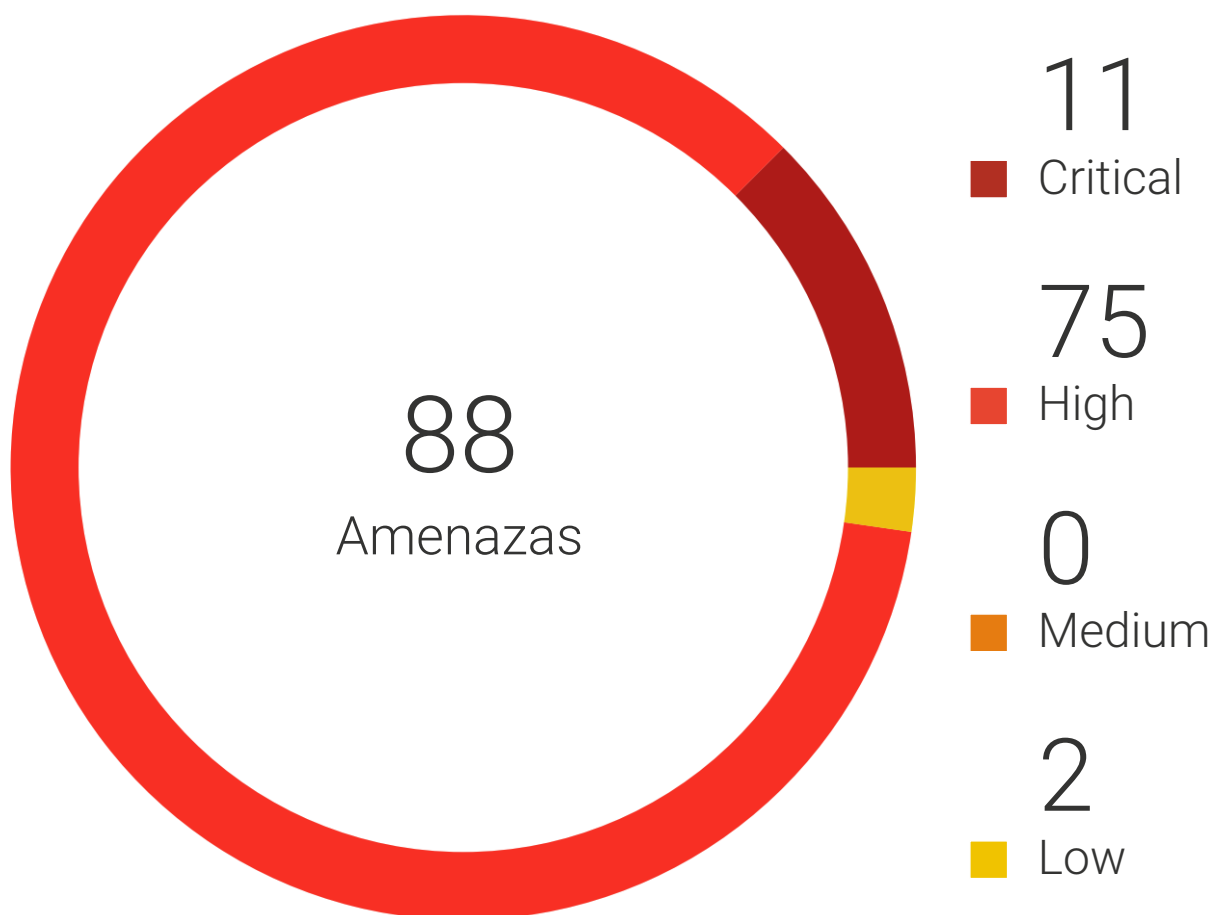
■ Low

# 9

## Amenazas por Host

## Host 81.25.000.00

En las siguientes páginas encontrará información sobre la severidad y la descripción de cada amenaza detectada por el host 81.25.000.00



**Threat ID: 30464 (Critical)**

Host: 81.25.000.00

Microsoft IIS WebDAV ScStoragePathFromUrl Buffer Overflow Vulnerability

Microsoft Internet Information Services is prone to a buffer overflow vulnerability while parsing certain crafted WebDAV requests. The vulnerability is due to improper validation of one of the headers, leading to an exploitable buffer overflow. A remote attacker could exploit this vulnerability by sending a crafted request to the vulnerable application. Successful exploitation could result in denial of service conditions or, in the worst case, arbitrary code execution in the context of the user running the application.

---

**Category**

---

**CVE**

CVE-2017-7269

---

**References**[https://github.com/edwardz246003/IIS\\_exploit/blob/master/exploit.py](https://github.com/edwardz246003/IIS_exploit/blob/master/exploit.py)

---

**Threat ID: 34221 (Critical)**

Host: 81.25.000.00

Apache Struts Jakarta Multipart Parser Remote Code Execution Vulnerability

Apache Struts is prone to a remote code execution vulnerability while parsing certain crafted HTTP requests. The vulnerability is due to the lack of proper checks on Content-Type in the HTTP request, leading to an exploitable remote code execution. An attacker could exploit the vulnerability by sending a crafted HTTP request. A successful attack could lead to remote code execution with the privileges of the server.

---

#### Category

code-execution

---

#### CVE

CVE-2017-5638

---

#### References

<https://cwiki.apache.org/confluence/display/WW/S2-045>

---

**Threat ID: 40007 (High)**

Host: 81.25.000.00

MAIL: User Login Brute Force Attempt

This event indicates that someone is using a brute force attack to gain access to mail server through smtp/pop3/imap authentication request.

---

**Category**

brute-force

---



**Threat ID: 40008 (High)**

Host: 81.25.000.00

MySQL Authentication Brute Force Attempt

This event indicates that someone is doing a brute force attack and try to authenticated to the MySQL server.

---

**Category**

brute-force

---

**Threat ID: 38865 (High)**

Host: 81.25.000.00

Oracle WebLogic WLS Security Component Remote Code Execution Vulnerability

Oracle WebLogic is prone to a remote code execution vulnerability while parsing certain crafted HTTP requests. The vulnerability is due to the lack of proper checks on payloads in HTTP requests, leading to an exploitable remote code execution. An attacker could exploit the vulnerability by sending a crafted HTTP request. A successful attack could lead to remote code execution with the privileges of the server.

---

**Category**

---

**CVE**

CVE-2017-10271

---

**References**<http://www.oracle.com/technetwork/security-advisory/cpuoct2017-3236626.html>

---

**Threat ID: 34605 (Low)**  
ZmEu Scanner Detection

Host: 81.25.000.00

This signature indicates that an attacker is trying to collect information about the network by using the ZmEu scanner.

---

**Category**  
info-leak

---

10

# Contacta con un asesor



### SW Girona

#### Data Center Salas 1 y 2

Edificio SW  
c/ Ponent, 13-15  
17458 Fornells de la Selva  
Girona

info@swhosting.com  
+34 972 010 550 tlf  
+34 972 010 555 fax

### SW Madrid

#### Data Center Sala 3

Edif. GlobalSwitch  
c/ Yécora, 4  
28022 Madrid  
Madrid

madrid@swhosting.com  
+34 918 137 825 tlf  
+34 972 010 555 fax

### ¿Necesitas ayuda sobre el informe?

Recuerda que puedes contactar con nuestros expertos en seguridad TI para recibir asistencia personalizada a la hora de interpretar el informe y sacarle el máximo provecho. Utilizando SW Panel podrás crear Tickets de Seguridad y te ayudaremos a solucionar todas las dudas o consultas sobre las incidencias y amenazas que hayan sido detectadas en este informe.