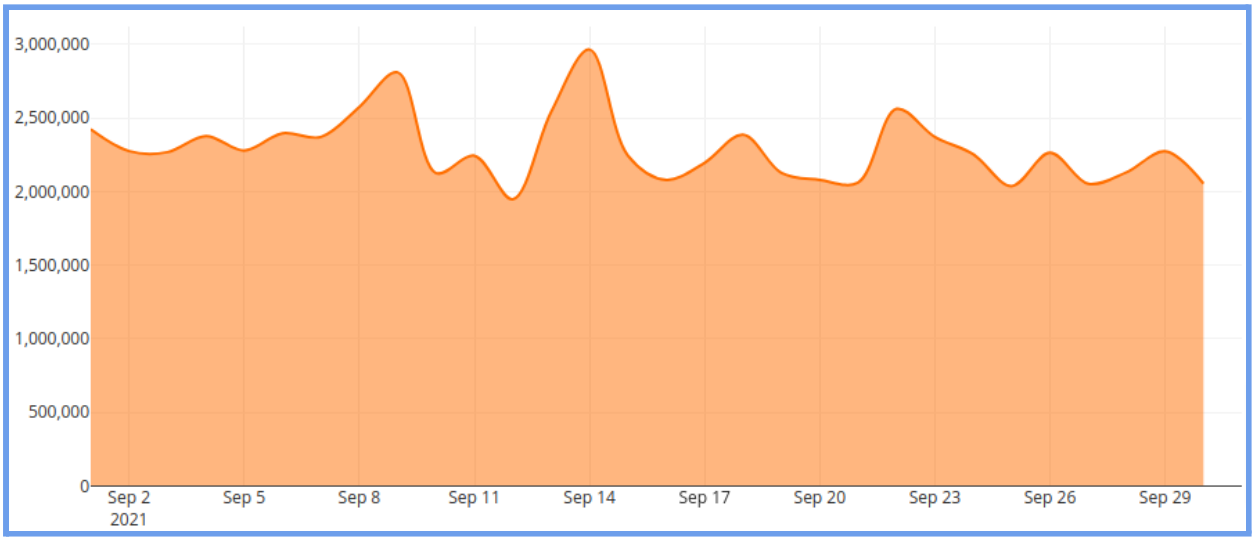
Reporte de actividad del proyecto

Despliegue de un IoT honeypot en América Latina y el Caribe

Septiembre 2021

Gracias a la capacidad de extracción de datos para la generación de reportes, se pueden reportar para este mes los siguientes resultados.

Actividad de registro de datos en el sistema



El día 14 hubo un un pico de actividad que llegó a cerca de los 3 millones de mensajes procesados, manteniéndose normalmente en un promedio ligeramente superior a los 2 millones. Los días 12 y 25 fueron los de más baja actividad, con un promedio de 2 millones de mensajes. Todo responde a un comportamiento normal.

Totales de mensajes y direcciones IP origen

Mensajes procesados:	Direcciones IP de origen:
68,740,762	619,484

Durante el mes se procesaron cerca de 69 millones de mensajes provenientes del proyecto de sensores, algo más de 6 millones menos que el mes anterior. Originados de casi 620 mil direcciones IP de origen distintas, alrededor del mundo, unas 30 mil menos en relación al mes anterior. Más abajo se desglosan estos orígenes por países.

Productos: Fabricantes y tipos más accedidos

Fabricante	Producto	Tipo	Eventos
Realtek	Realtek SDK	embedded-system	124363

Huawei	Huawei Home Gateway HG532	router	105430
MVPower	MVPower DVR	video-system	73152
Fortinet	FortiOS	firewall	72077
Microsoft	Exchange	email	19528
Dasan	Dasan GPON Home Router	router	18053
	Dasan GPON ONT WiFi Router H640X	router	2
D-Link	D-Link DIR-645, DAP-1522 revB, DAP-1650 revB, DIR-880L, DIR-865L, DIR-860L revA, DIR-860L revB DIR-815 revB, DIR-300 revB, DIR-600 revB, DIR-645, TEW-751DR, TEW-733GR	router	8518
	DNS-320	nas	4
Zyxel	Eir D1000	router	7939
Oracle	WebLogic Server	app-server	4828
	Oracle Weblogic Server	app-server	2456
MobileIron	MobileIron Mobile Device Management (MDM)	device-management-platform	4269
Realtek	Realtek SDK	embedded-system	124363
Huawei	Huawei Home Gateway HG532	router	105430

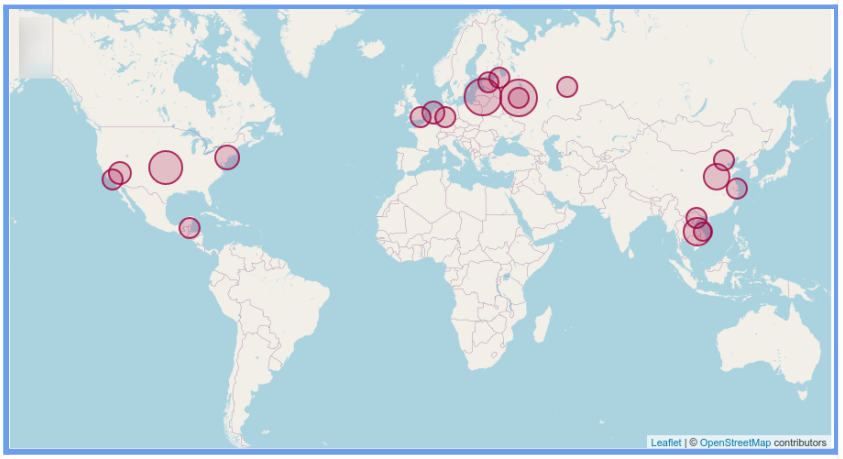
En el período, el sistema más asediado fue el sistema embebido Realtek SDK. Le sigue el gateway de hogar huawei HG532 y en tercer lugar, el sistema de video MVPower, aunque muy cerca está está el sistema firewall de Fortinet.

Países de origen de conexiones

Tabla de conexiones por país:

País	Conexiones
US	14844906
RU	10158791
LT	7470885
CN	6976492
VN	5542019
NL	3271865
DE	2726233
GB	1460430
IN	1293822

Representación Geográfica de orígenes:



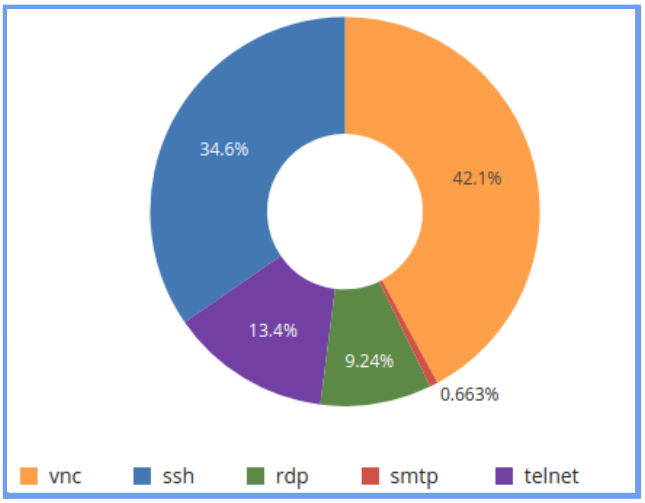
KR	1027009
BZ	837911
EE	734467
AU	725688
HK	703639
BR	666421
PA	573017
SG	551924
FR	540212
BG	490244
PL	463569

Algo más del 24% de las conexiones provinieron de EEUU, un 50% más que las de Rusia, siendo estos dos los que en total abarcan prácticamente el 41% de las conexiones tabuladas. Lituania está cerca de Rusia con poco más del 12% y le sigue China con el 11.43%. En LAC, Brasil destaca con el 1.09%, siguiéndole Panamá con el 0.94%.

💡 Es de notar que en el mapa no se representan todos los países de la lista tabulada, pues algunos países, como Estados Unidos, tienen geográficamente más de una ubicación (Ciudad) de origen, por lo que en el mapa se grafican sólo las 20 principales ubicaciones, no necesariamente consolidadas por país, que es lo que justamente se tabula a la izquierda.

Protocolos más accedidos

De las conexiones registradas, los protocolos que más se usan para acceder a los sistemas, son los representados en la siguiente imagen.



Cabe indicar que sólo se grafican los 5 primeros, pues a partir del 6to en adelante los valores realmente son muy pequeños, considerando que el propio protocolo SMTP en la gráfica (5to en presencia) sólo tiene un 0,66% de ocurrencia.

Usuarios y contraseñas más usados

Finalmente se presenta el top 20 de usuarios y contraseñas más comúnmente usados para acceder a los sistemas emulados por los distintos sistemas de honeypot en los diferentes sensores de la red:

Usuario	Ocurrencias	Porcentaje	Contraseña	Ocurrencias	Porcentaje
`root`	825020	65.01 %	`123456`	88705	19.57 %
`admin`	175292	13.81 %	`password`	46255	10.20 %

user	41538	3.27 %	**admin**	43344	9.56 %
default	25479	2.01 %	**1234**	40311	8.89 %
test	22335	1.76 %	**123**	34484	7.61 %
support	19560	1.54 %	**12345**	31871	7.03 %
guest	18787	1.48 %	**1**	21380	4.72 %
administrator	15413	1.21 %	**root**	16052	3.54 %
ubnt	13528	1.07 %	**12345678**	15787	3.48 %
postgres	12413	0.98 %	**test**	14836	3.27 %
web	12102	0.95 %	**user**	13069	2.88 %
admin1	12016	0.95 %	**123456789**	12015	2.65 %
user1	11089	0.87 %	**qwerty**	11096	2.45 %
ubuntu	10495	0.83 %	**pass**	10014	2.21 %
demo	10486	0.83 %	**1234567890**	9639	2.13 %
tech	10273	0.81 %	**1234567**	9614	2.12 %
oracle	8939	0.70 %	**7ujMko0admin**	8918	1.97 %
MikroTik	8286	0.65 %	**1111**	8880	1.96 %
profile1	8170	0.64 %	**default**	8835	1.95 %
telecomadmin	7815	0.62 %	**support**	8257	1.82 %